GORAMO- Janusz Górecki,
01-458 Warszawa, ul.Szańcowa 82
tel/fax (+4822) 877-39-94,
janusz.gorecki@goramo.com.pl,
www.goramo-gorecki.com.pl

MultiLink Router and MicroRouter

version 1.1.8

Warszawa, april 2010

1 ABOUT MULTILINK ROUTER AND MICROROUTER DEVICES 4

2 GETTING STARTED WITH THE DEVICE 4

2.1 SOFTWARE INSTALLED ON THE PURCHASE 4
2.2 THE STAGES OF START-UP 4
2.3 RUNNING THE SYSTEM WITHOUT AN RS-232 CONSOLE. 5
2.4 RUNNING THE SYSTEM CONNECTED TO THE RS-232 CONSOLE. 5
2.5 ESTABLISHING A CONNECTION TO THE RS-232 CONSOLE. 5
2.6 DEVICES CONFIGURATION 5

3 WORKING WITHOUT THE USE OF GRAPHICAL USER INTERFACE 6

3.1 HOW TO REMOVE THE GRAPHICAL USER INTERFACE? 6
3.2 HOW TO RESTORE THE GRAPHICAL USER INTERFACE ON YOUR ROUTER? 6
3.3 SAVING CHANGES TO FLASH MEMORY 6
3.4 INSTRUCTIONS FOR WORKING WITH A ROUTER WITHOUT A GRAPHICAL USER INTERFACE 7
3.5 PREPARATION OF THE ENVIRONMENT TO BUILD YOUR OWN, OR PROGRAMS DOWNLOADED FROM THE INTERNET 7

4 GRAPHICAL USER INTERFACE → GUI. 8

4.1 THE FUNCTIONALITY OF THE WEB INTERFACE 8
4.2 ACCESS TO THE GRAPHICAL USER INTERFACE 9
4.2.1 The Log over a web page / user name and password 9
4.2.2 Restoring the default password on a web page 9
4.3 INTRODUCTION THE CONFIGURATION BY WEB PAGE 10
4.3.1 Buton „Submit” 10
4.3.2 The buttons "Changes Apply" and "Submit & Apply" 10
4.3.3 Save Configuration to Flash, Write To Flash and Write & Apply. 10
4.3.4 Forms to enter setup 10
4.3.5 Form with the table 11
4.4 THE ORDER OF THE SETTINGS FOR THE ROUTER 11
4.5 GENERAL ROUTER SETTINGS 11
4.6 DEVICES TAB - CONFIGURATION OF PHYSICAL DEVICES 13
4.6.1 Configuring the router to work with interface V.35 and link E1/G.704 13
4.6.2 Configuring ports Eth0, Eth1, Eth2, Eth3, Eth4, Eth5 15
4.6.3 WLAN Configuration 15
4.6.4 Establishing a connection to an access point (Type: Managed) 16
4.6.5 Configuring the Access Point (Type: Access Point) 17
4.7 TAB INTERFACES - CONFIGURATION OF IP ADDRESSES 17
4.7.1 Configuring point to point 17
4.7.2 Configuring a Network 18
4.7.3 Downloading an address via DHCP 18
4.7.4 PPPoE Option 20
4.8 CONNECTION BRIDGE, CLUSTERING INTERFACES INTO BRIDGES 20
4.9 CONFIGURING MODEMS 21
4.10 CONFIGURING ACCESS GATEWAYS: GATEWAYS, COMPLEX GATEWAY (LOAD BALANCING) 22
4.10.1 Defining simple gateways. 22
4.10.2 Complex gateway 23
4.11 CONFIGURING ROUTING 24
4.11.1 Routing / Masquerading 24
4.11.2 Routing / Static Routes 24
4.12 SETTING UP REDIRECTS (PORT FORWARDING) 25
4.13 CONFIGURING THE FIREWALL 25
4.13.1 Blocking packets passing through a router 25
4.13.2 Blocking packets addressed to router 26
4.14 TRAFFIC MANAGER - LIMITING BANDWIDTH 27
4.15 QUALITY OF SERVICE - IMPROVING THE QUALITY OF SERVICE 28
4.15.1 Limitation "to lending". 28
4.15.2 Limitation " unchanging " 28
4.16 SERVICES "SERVICES" 28
4.17 USERS 29

4.18 GROUPS 29
4.19 STATISTICS 30
4.20 HOURLY STATISTICS 30
4.21 USER STATISTICS 30
4.22 TAB CONFIGURATION SCRIPT 30
4.23 SOFTWARE UPDATE GUI 32

5 MANUAL MICROROUTER TEXT MENU OVER THE CONSOLE (ONLY FOR MICROROUTER) 32

6 UPGRADING THE LINUX OPERATING SYSTEM 33

6.1 CREATE A COPY OF THE OPERATING SYSTEM AND CONFIGURATION SETTINGS 35
6.2 BACKUP AND RESTORE FEATURES 35

7 SAMPLE CONFIGURATIONS 36

7.1 SETTING UP A VPN CONNECTION 36
7.1.1 Connecting two LANs over one VPN tunnel 36
7.1.2 Details of the connection setup 38
7.1.3 Configuration "other" side tunnel 40
7.1.4 Additional information on the implementation of VPN 40
7.2 TRANSITIVE ROUTER 41

Introduction

Devices, which we describe are specialized computers designed for data transmission, in particular, to share Internet connections, using a variety of interfaces, both physical and virtual. The Linux operating system, used in these devices is especially breeds set of software instructions useful for data transmission. Construction of the device allows for independent changes to the operating system, or using the software package tested by GORAMO - Janusz Górecki. This document is a manual device. We strive to be transparent and useful as possible. We want to let both novice and advanced users to quickly start working with the router and the maximum of its use.

1 About Multilink router and MicroRouter devices

MultiLink and MikroRouter devices are actually full-fledged computers. The main differences between the PC and one of the devices are:

- A small amount of RAM;
- A small amount of embedded Flash memory, which contains the operating system;
- Comparable to Pentium 500MHz processor speed;
- Additional coprocessors permitting the network data transmission speed that far exceeds capabilities comparable to a Pentium processor 500MHz.
- In addition, of course, Multilink and MikroRouter devices consume significantly less power than even most economical PC.

2 Getting Started with the device

2.1 Software installed on the purchase

At the factory router has been installed in Linux Fedora operating system, with added software for configuration of selected functions over the website.

Please note that Linux and the GUI are separate components. The devices MicroRouter the text menu is also a separate element to run at logon to the system console.

You have the ability to remove additional software and work independently running the Linux operating system, or use operating system. Advanced users can certainly both.

To work independently with Linux it only has to master a few basic differences between the standard Linux operating system installed on a PC, and Linux installed on the routers and of course, be familiar with Linux operating system.

The main differences between the Linux operating system running on a standard PC, and Linux running on the router are presented in a later chapter, and due primarily to the limited amount of Flash memory and how to write files in memory.

To work with GUI, please refer to the section containing the instructions for use graphical user interface.

2.2 The stages of start-up

The system runs as follows:

- In the first place Flash memory is loaded with a program RedBoot, which manages the OS stored in Flash memory. Application RedBoot is small, it allows to repair the system in critical situations, or update the kernel and the file tree. Immediately after power-up, it just runs for 10 seconds and waits for the **Ctrl + C** sent from the RS-232 console
- If the operation is not interrupted by the **Ctrl + C** from the Flash memory operating system is unpacked and installed in a virtual file system in RAM. The system is running
- The operating system starts from a certain area of Flash memory - called configuration area - introduced changes are rewrite by the user and introduce into the system. These changes are the files that you recommended in the previous user to add or change the system

- After starting the system starts to load drivers that are usually installed at the time of recognizing through a router connected equipment, and during the devices detection (of course, even those built into the system). At the same time it is run script */etc/start*
- If in the router graphical user interface is installed, at this time the web server is started over command */etc/UI/scripts/applyChanges*. The consequence of this file is run, the server *busybox* is run too and the script */etc/UI/scripts/applyChanges* is executed
- If we are running MicroRouter, in the configuration, the file */etc/profile* contains command which runs the graphical user interface, whenever login is entered. Text user interface is run by the command: */usr/local/TextUI/start*

2.3 Running the system without an RS-232 console.

If you run a router, without RS-232 console, you should wait at least 60 seconds before the system starts. Only after a minute of power-system will be ready to work.

2.4 Running the system connected to the RS-232 console.

If during boot the console is connected to the RS-232 (in the MultiLink devices this is ttyS0, formerly Port A, and in the MikroRouter device this is port "Control"), it will be printed on any messages to her on stage of start-up.
In the first stage will run RedBoot, which for 10 seconds will be expected to press **Ctrl + C** - if we wanted to perform operations on Flash memory before starting the system. Then you will see a report from the boot completed application ready for work.
System ready asks for your password username and password. With the factory settings, you can log on to the user *root* by the password: *goramo1234*:

```
MultiLink login: root
Password: _
```

2.5 Establishing a connection to the RS-232 console.

To connect to the RS-232 console, use the HyperTerminal program, Putty for Windows or MiniCom for Linux, select the COM port on the computer connected to port A (MultiLink) or Port Control (MicroRouter) to configure the connection parameters:

The number of bits per second (Baudrate):	115200
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

Usually just enough to change the parameters of baudrate and flow control.

2.6 Devices Configuration

The device can be configured either using the graphical user interface (or a text interface for configuring the bridge mode in MicroRouter), or independently by means of self-generated scripts. Both have their advantages and disadvantages. An advantage of self-configuration is practically decoupled from the limitations of the graphical user interface and full control over the device. After learning to work with a router, it is nice and fast. This method is recommended for people who have experience in configuring Linux.
The advantage of the graphical user interface is that it does not need to get acquainted with Linux, the device can configure the Web browser. The graphical interface lets you configure the basic functions, but is constantly adds new possibilities.

3 Working without the use of graphical user interface.

Do not be afraid to work without the use of graphical user interface. If tempts us to this thing to work with the router, you can only encourage this. First, just in case, we should learn to connect to the router via RS-232 cable (See: 2.4, 2.5), and then removing the graphical user interface and start implementing changes / configuration commands to the file */etc/start*.

If we determine the connection with RS-232 will be able to recover the web interface, if such a need arise.

3.1 How to remove the graphical user interface?

To remove all the extra software that came with the router - apart from the "clean" operating system - we need to delete the contents of */etc/config-files* files and run command *write-config*. Memory containing the configuration files will then be completely cleared. It will also erase all of the additional router configuration. However, remember that when you restart you will not be able to get the router via SSH console since the factory settings Ethernet ports will be removed. To avoid this in */etc/start* file should delete the three commands which runs graphical user interface

```
/etc/UI/scripts/initializeUI
/usr/local/WebGUI/start
/etc/UI/scripts/applyChanges
```

and add commands loading drivers for Ethernet cards, configures Ethernet port and a trigger SSH server:

```
modprobe ixp4xx_eth
ifconfig eth0 192.168.0.222/24
/sbin/sshd
```

If we do not we will have to get to the device through the RS-232 console.
Similarly, if you do not write down passwords and pre-generated the network keys that identify router (to connect via SSH). In the file */etc/config-files* we have put entries

```
/etc/start
/etc/shadow
/etc/ssh\_host\_dsa\_key
/etc/ssh\_host\_dsa\_key.pub
/etc/ssh\_host\_rsa\_key
/etc/ssh\_host\_rsa\_key.pub
```

and execute the command:

```
write-config
```

When you restart your system after the graphical user interface on the router will not sign and we will have access to the device through SSH console.

3.2 How to restore the graphical user interface on your router?

If the router has no graphical user interface, and we would like to use it, we could record it, after fetching the complete GUI from *http://goramo.com.pl/public/WebGUI/*. Archives should be placed on the router in the */tmp/* catalog, unpack and make the software installation using a script *install_release* inside the archive:

```
tar xzf install_0_8_2en.tgz
./install_release
rm install_0_8_2en.tgz
```

After these commands, you can either save the changes to Flash memory, by the command */etc/UI/scripts/saveChanges*, or by a Web page - select the *Write To Flash*. Next, restart the router.

3.3 Saving changes to flash memory

The operating system is run from a virtual file system in RAM. Changes in the system files remain in RAM until you reboot. To save changes permanently, you must save them in the flash memory area called the configuration area.

List of changed or added files or directories should be placed in */etc/config-files* and run a *write-config*. Selected files (and directories) will be compressed *tar* command and placed in Flash memory. Please note that this file is usually already includes a list of files and should be preserved. Inclusion on the list of directories will save all of its subdirectories and files contained in it. Advanced and more inquisitive users can read the script */bin/write-config*.

3.4 Instructions for working with a router without a graphical user interface

We need to know exactly how to save files on your router (please put a list of changed or added files or directories in */etc/config-files*, then save the changes by the *write-config* command.) To edit files on the router, is available only to the vi editor, which many users is considered as a tool for a very uncomfortable (however it takes little space in Flash memory). It is recommended, so keep the changed files on the local computer where the changes are made convenient editor - and copy changed files to the router command *scp* (Linux) or *WinSCP* (Windows). Please note that the configuration files contain these Linux (not Windows) marks the end of the line (for this reason, we recommend editing under the Linux operating system).

Another convenience can be placed in */etc/config-files* permanent inscription */etc*, which will cause the all contents of */etc* directory will be saved. This removes the need to change the contents of file */etc/config-files* each time you want to add or remove a configuration file located in the */etc* directory (please note that in point: "How to remove the graphics?" specially to */etc/config-files* write down list of files that have changed - to all files and changes related to the GUI */etc/UI/** some versions of */etc/profile* was deleted.)

3.5 Preparation of the environment to build your own, or programs downloaded from the Internet

On the router you can run all the programs available for Linux. The problem is that each of these programs require compilation. On the router, of course, you have not installed the compiler (because of the small amount of flash memory), but the environment to compile programs in a way that they operate on the router - can be prepared on any computer. Of course, we recommend that this was a fast computer.

To prepare the compile environment should download the appropriate compiler, and fragments or wide software available online (at the Open Source license - the GNU), or from the company Goramo. Before we do that lets settle the directories in which will be placed the newly installed components:

/usr/local/xscale_be	A local copy of the main tree router system;
/usr/local/host-tools	Tools for compilation;
~/multilink-devel	The directory in which we store files downloaded from the Internet

Create folders and retrieve archives:

```
mkdir ~/multilink-devel
cd ~/multilink-devel
wget http://www.goramo.com.pl/public/binaries/gml-sysroot-20080228.tar.bz2
wget http://ftp.gnu.org/pub/gnu/binutils/binutils-2.17.tar.bz2
wget http://ftp.gnu.org/pub/gnu/gcc/gcc-4.1.2/gcc-4.1.2.tar.bz2
wget http://www.goramo.com.pl/public/sources/gcc-4.1.2-no-usr.patch
wget http://www.goramo.com.pl/public/sources/gcc-4.1.2-arm-be.patch
```

Unpack the main tree sysroot, which will allow us to GCC compilation:

```
cd /usr/local/xscale
tar xjf ~/multilink-devel/gml-sysroot-20080228.tar.bz2
```

Unpack the source binutils and compiler, and then proceed to compile:

```
tar xjf binutils-2.17.tar.bz2
tar xjf gcc-4.1.2.tar.bz2
```

Compiling binutils and GCC. Directory with the tools to at least GCC compile time we need to add the path. Tools put in directory `/usr/local/host-tools`:

```
export SYSROOT=/usr/local/xscale_be
export TARGET=armeb-pc-linux-gnu
export PREFIX=/usr/local/host-tools
cd binutils-2.17
./configure --with-sysroot="$SYSROOT" --target="$TARGET" --prefix="$PREFIX"
--disable-nls --
make
make install
cd ..

cd gcc-4.1.2
export PATH=/usr/local/xscale_be/bin:$PATH
patch -p1 < ../gcc-4.1.2-no-usr.patch
patch -p1 < ../gcc-4.1.2-arm-be.patch
./configure --with-sysroot="$SYSROOT" --target="$TARGET" --enable-
languages="c,c++" --prefix="$PREFIX" --disable-nls
make
make install
```

At this point we are in the directory:
`/usr/local/host-tools`
tools to compile in the directory:
`/usr/local/xscale_be`
tree with "includs" and router static libraries.
For projects compiled externally adding the appropriate flags. For example, wanting to compile *Lighttpd* server run the compilation with the parameters indicating the use of compiler */usr/local/host-tools*:

```
tar xjf lighttpd-1.4.15.bz2
cd lighttpd-1.4.15
CFLAGS="-D PATH_MAX=8192 -I/usr/local/xscale_be/include"
LDFLAGS="-L/usr/local/xscale_be/lib"
CC="/usr/local/host-tools/bin/armeb-pc-linux-gnu-gcc"
export CFLAGS LDFLAGS CC
./configure --host=armeb-pc-linux-gnu
make
make install
```

4 Graphical User Interface → GUI.

4.1 The functionality of the Web Interface

Currently, the graphical user interface allows you to:

- Configure your router to work with the link protocol HDLC Frame Relay or G.704
- Configure your router to work with a link Cisco HDLC protocol
- Configurations Ethernet ports eth0 and eth1 to work with different MAC addresses in different modes
- Allocation of network interfaces one or more IP addresses and subnets
- Log PPPoE interface Eth
- Setting the masquerading between gateway and networks indicated a network interface
- Running DHCP server networks operating on the specified network interface
- Setting port forwarding to the designated internal computer network
- Setting the basic principles of firewall
- Create a VPN encrypted connections
- Introduction of scripts by the web page to implement a configuration that can not be implemented at the moment by the web page

- Software Update GUI
- Load Balancing (bookmark *Complex Gateway*) between defined Internet gateways
- Connecting to the network interfaces in a bridge connection
- Setting up a wireless network

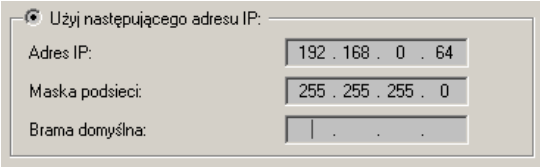
The graphical interface is not share at the moment all the possibilities of the router.

4.2 Access to the graphical user interface

At the moment on the run router is available RS-232 console, with standard goramo1234 password for user root, and are configured Ethernet interfaces from eth0 to eth5 depending on the version of the device.

Eth0 port is assigned an IP address 192.168.0.222. Eth1 port is assigned an IP address 192.168.10.222. Both ports are prepared to work in the subnets specified mask of 255.255.255.0.

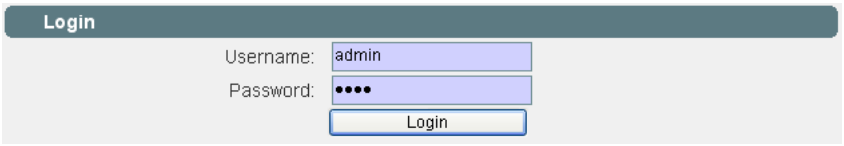
To connect to the web through the port eth0 router must be configured on a PC network, which we want to operate the device, giving it an IP address pool of 192.168.0.1 to 192.168.0.254, other than the address 192.168.0.222, and set the subnet mask 255.255.255.0.



4.2.1 The Log over a web page / user name and password

When you connect your computer to the router, open a web browser and type the router's IP address preceded by the name of the protocol http:// in the address box:

The browser will open the login page of the router. To start the configuration we need to enter the ***admin*** username and standard password ***goramo1234***.



Once you log, in the browser window appears on the software version information recorded on the router, and a version of the device.

4.2.2 Restoring the default password on a web page

Please note that the console password for the root user is a different password than the password on the web page. No password can not be read, but being able to log into a web page we are able to reset the root password, and vice versa: logging into the console and issuing the command:

```
rm /etc/UI/webpassword
/usr/local/checkconf fix
```

restore the default password Web pages, user admin. In general, way is to delete the configuration file with a password Web site and run repairer program for deficiencies in the configuration web page. The program will restore the default contents of the file.

4.3 Introduction the configuration by web page

Note that the settings from a Web page are first placed into the cache device (called RAM) and only then can be put to use and saved to flash memory. Despite appearances, this division is to facilitate the configuration of the router and allow extrication with a number of embarrassing situations.

4.3.1 Buton „Submit”

Placing configuration to the RAM is in practice a form of submitting the contents of Web pages to the router. It is performed after clicking on "Submit." In this way the configuration is sent to the router physically, but will be lost when the power cut, or restart the computer. There is not also still active.

4.3.2 The buttons "Changes Apply" and "Submit & Apply"

To activate it, select the button "Apply Changes",„*Apply Changes*”. Separation of these activities may be very useful when configure the router remotely. Imagine a situation when you want to eg change the IP network interface through which we have established a connection to the router. After this change the connection is broken. Of course, we can connect again, but change the IP address and gateway, which uses a router, when you try to configure the external network is impossible.

Obviously in cases where the immediate does not prevent us to use the settings we wish to comply with both settings by selecting the *Submit & Apply* and it is most likely done option. *Submit & Apply* button is available in every form to enter setup, next to the Submit *Submit* button, because the operation is a natural continuation of *Apply* operations on *Submit*. *Apply Changes* button is available on the left side of the Web. Is placed under the main menu web page and is visible only when the Web configuration changes are implemented in RAM, which have not been put to use..

4.3.3 Save Configuration to Flash, *Write To Flash* and *Write & Apply*.

The next step is to save the changes to Flash memory. Record setup takes about two minutes, and perform it every time you introduce a change would be inconvenient. In addition, the implementation of this stage late usually allows us to check the setting before their final implementation. Introducing restrictive firewall settings we are sure that when the lock yourself access to the router, just turn off the power at the moment to return to the setup, which recently allowed us to get to the router. Flash memory configurations to be written by pressing the *Write To Flash* is under the main menu web page. If you are sure that once introduced the configurations you want to save (or, for example by introducing it to lose connection to the router, but we are aware of) we can use the *Write & Apply* button, which first introduces the configurations introduced into RAM and then writes it right away in Flash memory.

Write to Flash button is available on the Web at left menu. Is visible only when the RAM is placed on changes that are not stored in *Flash* memory. *Write & Apply* button is available only if the changes introduced to RAM have not been put into use, or stored in Flash memory.

4.3.4 Forms to enter setup

Entering configuration consists primarily of filling out forms. To facilitate the configuration of all Web forms are maintained in the same convention. Any form is responsible for a certain area and under every configuration form is available, there are two buttons: *Submit* and *Submit & Apply*. As already explained, are responsible for sending the configuration from a Web page into RAM, in order to introduce it to use or save to flash memory in convenient time, or while sending them to the memory and process usage.

Each consists of a list of fields to configure. In every field we can select an interesting value. Changing values in a field configuration may hide, or change certain options form (irrelevant options are hidden.)

4.3.5 Form with the table

Under some forms, is placed a table and the form for editing the contents of the table. The form for editing the contents of the table is placed in a dark green rectangle. By default, in this form for editing the contents of the table is a button "Add Row" which choose to add a new row at the end of the table or "Update Row", which introduces changes to the currently edited row table.

To access the form editing selected row, press the "Edit" button on the right side of our interesting line in the table. To access the form for adding a new row at the end of the table, click on the link "Add New Row" button just above the table.

4.4 The order of the settings for the router

First, it is recommended to configure all network devices (Devices tab and Modems tab), of which the router will use when working. After the device configuration should be given the IP addresses of network interfaces (tab Interfaces) from which you will use. After setting the network interfaces should be access to the Internet gateway (gateways). The router must have access to any of them. In the *Interfaces* tab, you can check us interesting interfaces have no problems with the reception of the media (no flag-NO CARRIER).

Only after the above steps and configuration, go to the configuration of Routing and Firewall advanced settings. At the end do you change your password to access the Web, and change the password to access the console as user *root*.

4.5 General Router Settings

Tab General Settings allows you to configure options related to the behaviour of the router. Included here are the settings related to access to the router settings, network router settings, other than the IP addresses that are configured in the Interfaces tab, such as the name of the router on the network, DNS addresses from which the router can use, the address of time server and gateway, the router can use, if he wants to connect to the Internet (for example, to retrieve current time).

A detailed description of all available options is included in the table.

option	description and use
Router Access	Access to the router settings. In this section, we set - how you can get to the router
Enable SSH	This option determines whether the router is running as the SSH server that allows remote login to the router console (Secure Shell). Switch off this option if you do not intend to log on to the console and change the default password assigned to it. Attention! Password for the console is set by the console, you can not change it from the Web interface.
Hostname	The network name of the router. The name under which the router will be visible on the local network.
System's Gateway	The system gate. The access to the Internet Gateway, which uses a router. The router sends queries virtually only the current time, to the time server in the "Time Server IP
SSHD Port Numer	The port number on which Secure Shell server (SSH) is listening on the for remote connections to the console. The default is port 22, destined for this service, but the administrator may change the port number to avoid conflict or obstructing access to the router .
WebGUI Port Number	Port number on which Web site is made available to the router. The default is port 80, which is the standard port number for HTTP service. Just as with SSH port, number can be changed by an administrator.
Router's DNS and domain	Setup your domain name and DNS
Primary DNS	The main DNS server. The router uses this computer (the computer on a specific IP address), to replace the name of the URL to an IP address. NOTE: This field can currently enter the following values: -Specific DNS server IP address -Value "MODEM_ <modem ID> _DNS1 -Value "MODEM_ <modem ID> _DNS2 The first entry indicates a specific DNS server, the other two entries specify the appropriate server addresses DNS primary / backup DNS received by the specified modem to connect to the provider. NOTE: Important information is that these IP addresses (referred to here), you can refer to when setting up DHCP servers. The address in the Primary DNS as the General Settings tab describe as: MAIN1
Secondary DNS	Backup DNS server. Field work exactly as Primary DNS, is used only when the router can not contact the Primary DNS server, and in other settings - you can refer to this field and enter the value MAIN2 (only where such an appeal makes sense - that is, couple asked to enter the DNS server address)
Domain	Setting Domain; makes an entry Domain to the file /etc/resolv.conf
Date and Time	Date and Time
Time Server IP	The IP address or name (if given the DNS in previous point) server from which to download the current time
Time Zone Modificator	Changing the time, to modify the time zone. In most cases this option is not needed, because time and change time zones into account the time server. For the current time taken from the time server is added to the appropriate (which may be negative) the number of hours.

Because these options affect the operation of the system under them is the possibility of introducing them to the configuration without the introduction of the use (*Submit*), or the introduction and immediately approve a new configuration (*Submit & Apply*).

Language Options	Language settings
Language	Choosing the language in which the GUI is displayed. The choice of language will be approved immediately click Submit & Apply. The main language used is English. Supported is also Polish, Russian language support we planned.

On the tab you can download the configuration of the router. Configuration is stored in a file router_config.tar.gz (archive). The file can then be recorded on the same router to recover the configuration, or recorded to another router, such as a replacement / backup. Download a configuration by clicking on the link "Download Configuration File." We download configuration options for selecting the file by clicking on the drive (the download link"') - a description depend on the browser button, then click on "Send File".

Change Web Page Administrator Password	
Current Password	current password
New Password	new password
Confirm Password	confirm password

To change the password for user "admin", enter your current password, then enter the new password twice (enter and confirm) and choose *Change Password*.

The last option lets you reset your router if you can not turn it off. To reset the router to select the last button "Reboot System".

4.6 Devices tab - configuration of physical devices

This tab is visible physical devices that are not modems - installed in the router. These include:

- the Ethernet ports (two to four, or more if there is connected via USB)
- the HSS device, shown as HDLC0 and HDLC1
- a wireless network card is WLAN0, if installed in the router

This tab allows you to configure the physical transmission parameters closely associated with a specific interface, such as speed, operating mode. Device settings can affect the network interfaces available on the Interfaces tab.

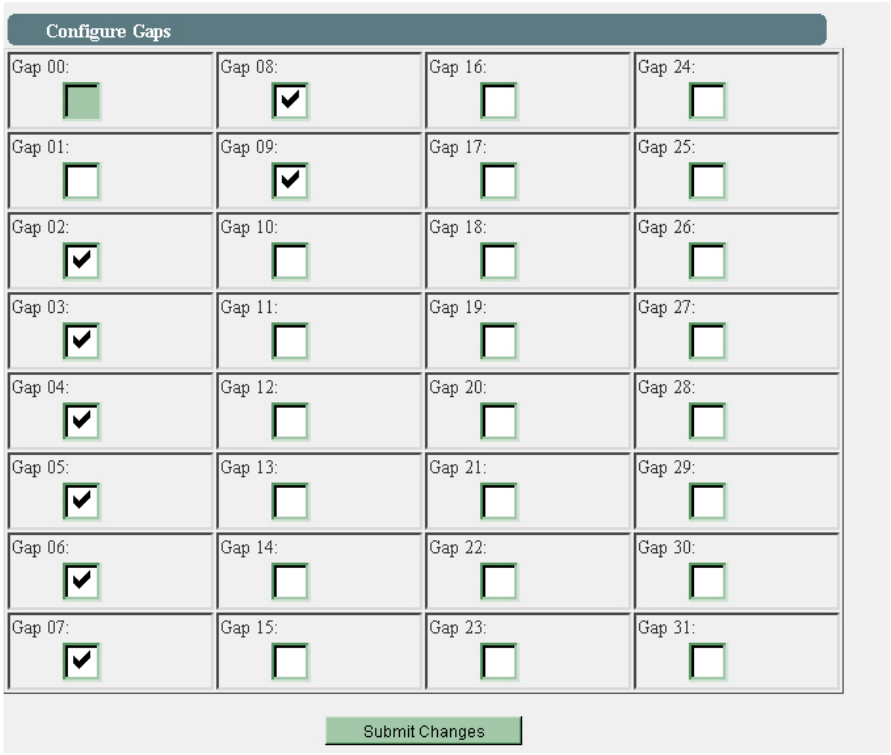
4.6.1 Configuring the router to work with interface V.35 and link E1/G.704

Routers are usually equipped with two HDLC links marked HSS0 V.35 and HSS1 V.35. Operating parameters, configure the port through the *Devices* tab. After entering the *Devices* tab in the *Operation Mode* field, select HDLC mode displays a list of devices that can configure the device comprising hdlc0 and hdlc1. Select the device that you want to configure and click on the *Configure* link on the right side of the table.

When you select *Configure* you will see a form with specific configuration parameters HDLC port. The first two are the *Clock Rate* and *Protocol*. The next option that will be displayed depend on the options *Protocol* setting.

Option	Clock source /protocol	Meaning
Clock source	External	Router synchronizes with the clock received from the link supplier
	Internal	Router generates a clock (signal sync) allows data transfer speeds with any of the range of 64 to 22,000 kbps (maximum rate of speed is the sum of two channels, ie if first channel will have a speed 10Mbit/s, the second can only have 12Mbit/s)
Protocol	Frame Relay	Port HDLC (HSS) is used to work in the Frame Relay network (the network is characterized by high bandwidth, organized by Frame Relay protocols and recognized as an open standard). When you select this option we can choose the settings described in section 7.2.2.
	Cisco	Port HDLC (HSS) is used to work in network organized by protocols developed by CISCO.
	Hdlc-eth	HDLC port will be configured to connect two Ethernet network via the serial port HSS.

After selecting the appropriate Cisco or Frame Relay protocol we can still give its performance. For Frame Relay protocol, very important is to create a channel DLCI. Example HDLC Configuration with HDLC Protocol, see the examples under the title Setting POLPAK-T connections.
If you have a router with interfaces G.704 marked **E1_0** and **E1_1** to the options described above, there is one more: G.704 route configuration slots. In the *Operation Mode* field, select G.704 and then *Configure Gaps* and select the slot in which transmission is to take place. If you want to use the link in a transparent mode G.703 in the field *Operation Mode* HDLC option should be left.



4.6.2 Configuring ports Eth0, Eth1, Eth2, Eth3, Eth4, Eth5

Please note that the Ethernet ports usually do not require additional configuration. Of course, the operation should not be confused with the configuration of network interfaces eth0 and eth1, etc.

Routers are equipped with a number of Ethernet interfaces. Number of interfaces ranging from one to six[1], depending on the version of the router. For each of the built-in network interfaces, we can determine the MAC address and mode of operation - defining the speed and mode of action of the interface (at the moment does not apply to the interface connected to the USB port). If you do not want to set your own MAC address for Ethernet interfaces, the interfaces will use MAC addresses from the pool reserved by GORAMO.

To configure these settings, go to the tab *Devices*, and in the line representing interests us interface on the right side of the to select the *Configure* tab. You'll see a form with the following parameters:

Current MAC Address	---	Currently assigned MAC address
Overwrite MAC Address	[X]	The question is whether we want to overwrite the factory MAC address
MAC Address	00:00:00:00:00:00	This field allows you to enter the MAC address, which if you select *Overwrite MAC Address* is replaced by a factory address.
Media Technology	All enabled	Interface negotiates optimal (fastest) mode
	Force 1000 Base T Full Duplex	Force 100Mbits, Full Duplex
	Force 1000 Base T Half Duplex	Force 100Mbits, Half Duplex
	Force 100 Base T Full Duplex	Force 100Mbits, Full Duplex
	Force 100 Base T Half Duplex	Force 100Mbits, Half Duplex
	Force 10 Base T Full Duplex	Force 10Mbits, Full Duplex
	Force 10 Base T Half Duplex	Force 10Mbits, Half Duplex

NOTE: If you use optical interfaces eth0 and eth1, manually select a field value of "Media Technology" as Force 100 Base T Full Duplex.

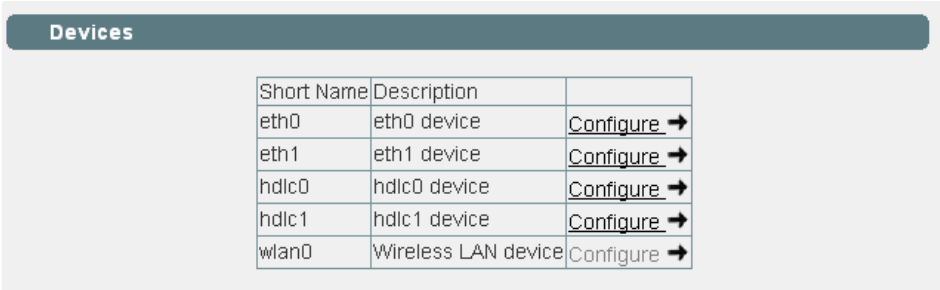
For all the Ethernet interfaces you can enter your login with the username and password PPPoE, and of course IP addresses. These settings are available from the Interfaces tab.

4.6.3 WLAN Configuration

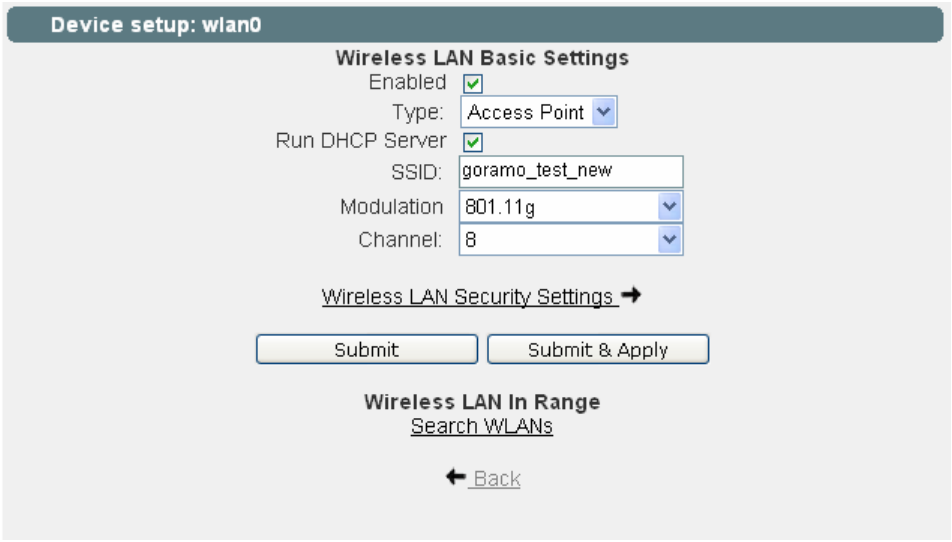
The device allows the WLAN configurations, if they are connected to his WiFi card. When you connect your WiFi in the tab *devices* appears the WLAN0 device and in the *interfaces* tab interfaces WLAN0. Connecting the next WiFi devices will result in the appearance of interface *wlan1*, *wlan2*. At present, there may be problems with the order of equipment (eg remove the device wlan0, wlan1 device is renamed wlan0).

WLAN device visible under the name wlan0, we can set up after clicking „*Configure*" in the line representing the WLAN *Devices* tab.

[1] Eth 4 and 5 are based on internal PCI bus. If you need even more ports Eth, it can be obtained by connecting a USB converters: DUB-E100 F my D-Link. "



After clicking on the button "Configure" on the right side of the device wlan0, go to the tab that configures the wireless card:



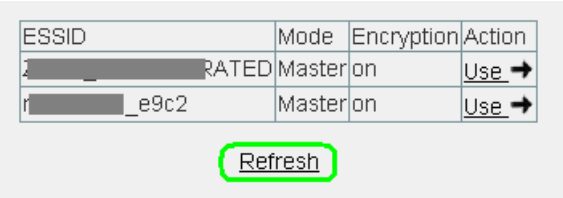
The current setup allows us to configure the device in the mode:

- Access Point - Point of access mode in which the router provides wireless computers within range of your network card.
- Managed - a mode where the router wants to connect to a wireless network.

In each of these modes the router requires settings (or download automatically from the existing access point) network parameters. At present, the parameters for settings are: SSID, network card modulation and the frequency (channel) on which the signal is transmitted.

4.6.4 Establishing a connection to an access point (Type: Managed)

In the case of network Managed the router can retrieve these parameters. At the bottom of the tab is the option "Search WLANs," which displays all available for the router wireless networks. The list of available wireless networks when you click "Search WLANs" will be displayed on the configuration, together with the possibility to refresh the list.

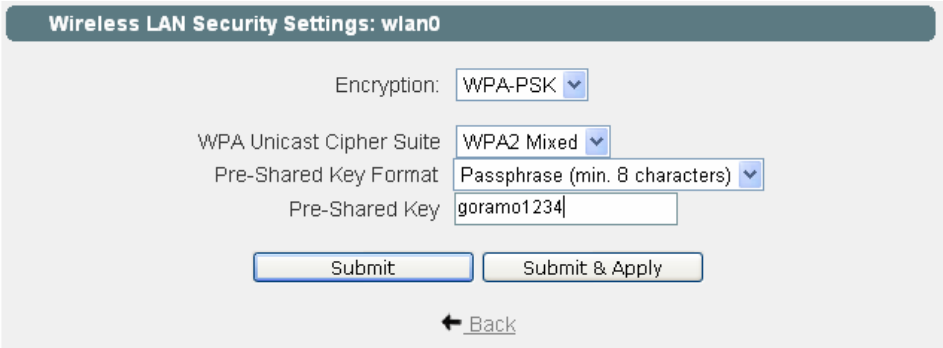


On the right side of each wireless network that appears is a button that allows you to rewrite the parameters for configuration.
After completing the setup and select the "Submit & Apply" wireless network connection is established.

4.6.5 Configuring the Access Point (Type: Access Point)

If you want to configure the access point for the router:

- enter the *devices* tab
- select the network adapter configurations: wlan0, by clicking "More"
- in the network card configuration:
  - option Type in the configuration set to Access Point
  - in the SSID field, type the desired wireless network name
  - if we set / change the modulation (default 801.11g)
  - choose a free channel on which will be running the wireless network and change the channel parameter.
- Select the option "Submit" to save settings for your wireless card (not on "Submit & Apply", because this option would run the network before security settings)
- Set security:
  - click on the "Wireless LAN Security Settings" option
  - choose the parameter Encryption WPA-PSK (default None, None setting switch off security)
  - choose method of security (two types of WPA and WPA2 one), choose the safest option is WPA2 (WPA2 Mixed))
  - choose the form of a password, or at least 8 character string, or 64-bit number hexagonal
  - write down the root password (Pre-Shared Key)
  - select the "Submit & Apply" which will cause the settings.



4.7 Tab interfaces - configuration of IP addresses

After setting up the equipment and modems, they are represented by the network interfaces. Available interfaces are presented on the *Interfaces* tab.
After clicking on the option "More" on the right side of the line representing the network interface we are interested, go to the configuration details.

Enable Interface	if the interface is to be run
Configuration Type	to choose: Network or Point to point

Each interface can operate as an interface to multiple computers on a network, or interface that combines elements of only two computers. Of course, with each interface between two computers can also be configured as a network interface (Configuration type: network).

4.7.1 Configuring point to point

Setting up a network of point to point is less interesting. Set in its IP address on the router (Local IP) address of the computer and on the other side of the link (remote IP). Setting the mask is not used in practice. Best to leave the value of 255.255.255.252

4.7.2 Configuring a Network

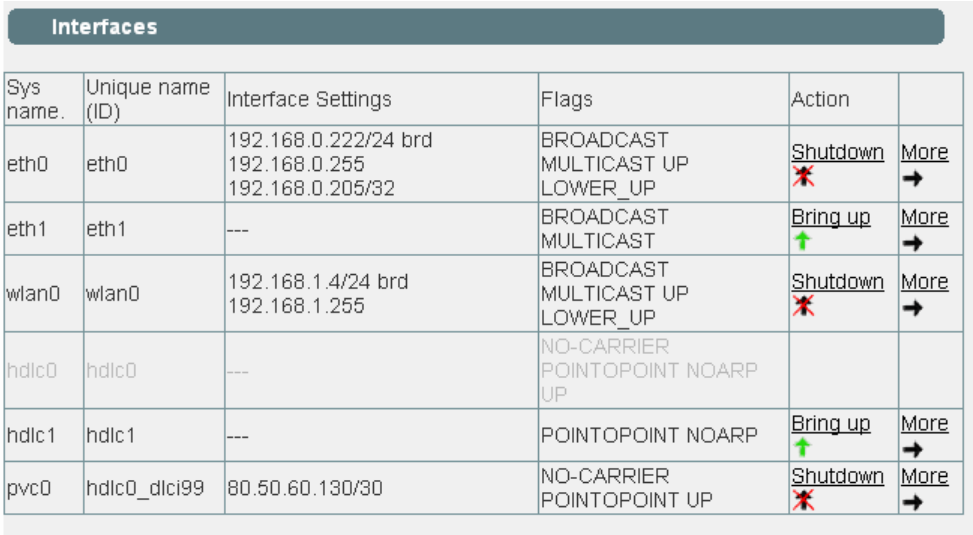
Network configuration is a standard type of IP address configuration. In this configuration, the address may be automatically assigned by the DHCP server (Please choose option Enable DHCP) or manually entered.
If the address is automatically assigned by DHCP does not need to set the remaining fields (the settings are not relevant.) After entering the configuration to use - try to get the address of the router interface from a DHCP server. If it succeed - the address will be checked on the *Interfaces* tab. If it fails - the *Interfaces* tab of the interface is running, but will not have an IP address. If you assign the address manually fill in the following fields:

ip address	main IP address (eg. 192.168.0.222)
net mask	net mask (eg. 255.255.255.0)
virtual IP 1	first additional IP address, together with a summary given netmask (eg 192.168.0.40/24). If the field does not interest us - leave set to 0.0.0.0.
virtual IP 2	second additional IP address, ibid.
virtual IP 3	Ibid.
virtual IP 4	Ibid.

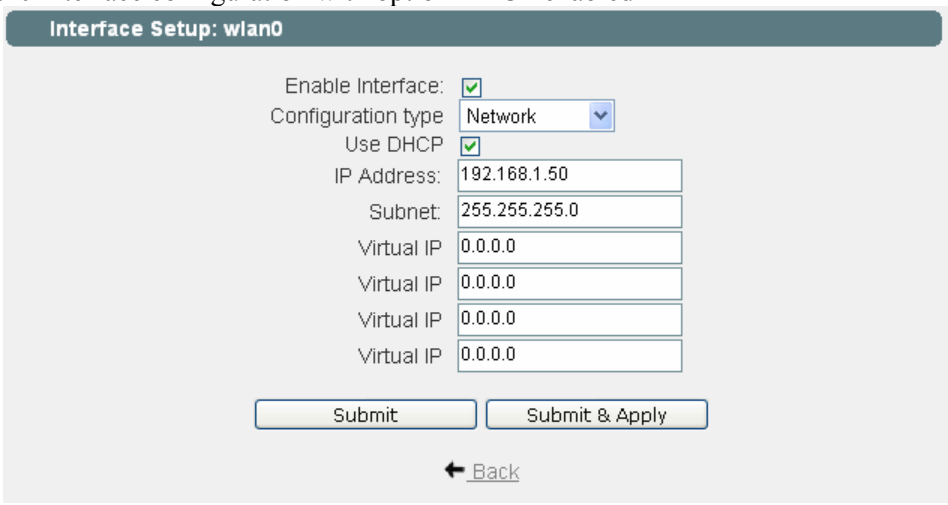
4.7.3 Downloading an address via DHCP

If you need to download the settings from the DHCP network Server, in the configuration interface, select Configuration Type: Network (default) and select option Use DHCP. At the time of approval of changes to the interface will automatically be assigned an IP address assigned by the DHCP server (If the connection succeed) Additionally, in other parts of the configuration (examples attached below) will be able to use the shortcuts:
DHCP_gw_xxx – shortcut for gateway specified by the DHCP server for interface xxx
DHCP_dns1_xxx – shortcut for the address of primary DNS server specified by DHCP for the interface xxx
DHCP_dns2_xxx - secondary server DNS specified by DHCP

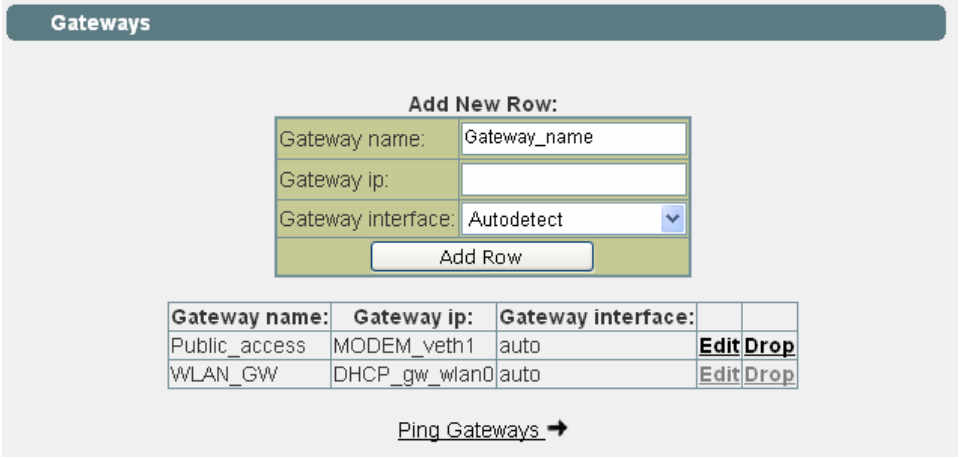
View tab interfaces.



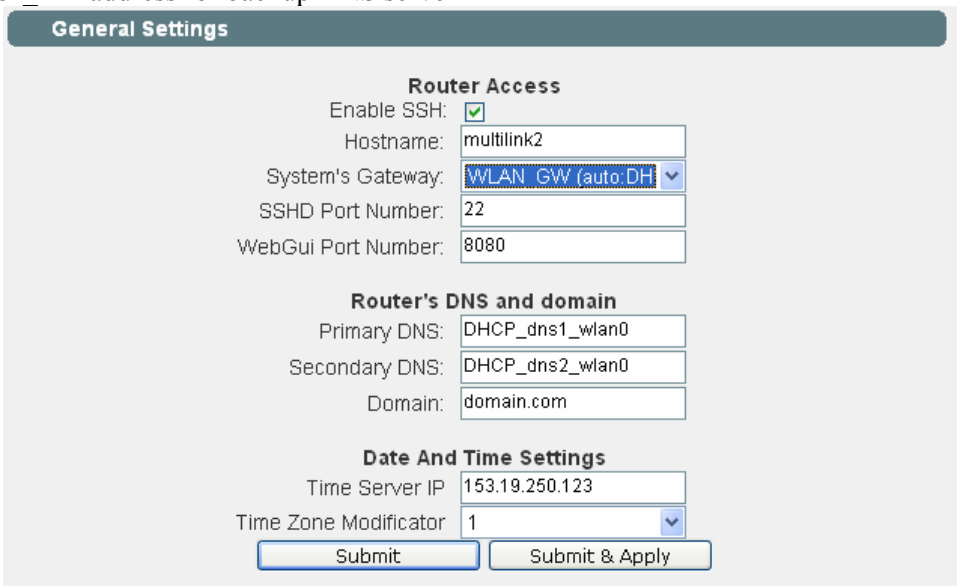
Details wlan0 interface configuration with option DHCP enabled



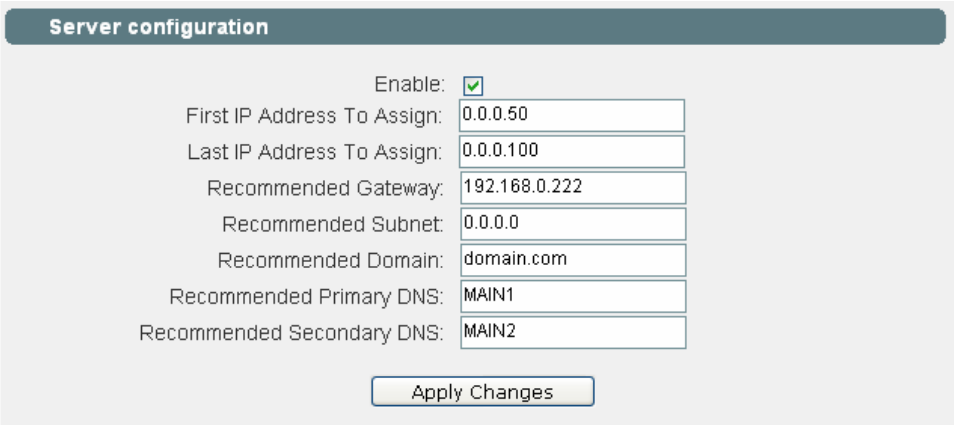
On the Gateways tab, instead the IP address of a specific type: DHCP_gw_xxx, where instead of xxx type the name of the network interface, that uses DHCP.



On the tab General Settings (General Settings) in the "System's Gateway" to select previously defined gateway. Instead of using a DNS address identifiers:
DHCP_dns1_xxx for main DNS server address
DHCP_dns2_xxx address for backup DNS server



Similar shortcuts you can use to configure the DHCP server that supports our local network. In fields Recommended Primary DNS and Recommended Secondary DNS entries can be made:
DHCP_dns1_xxx
DHCP_dns2_xxx
or wanting to use the addresses defined in the General Settings tab, respectively
MAIN1:
MAIN2



4.7.4 PPPoE Option

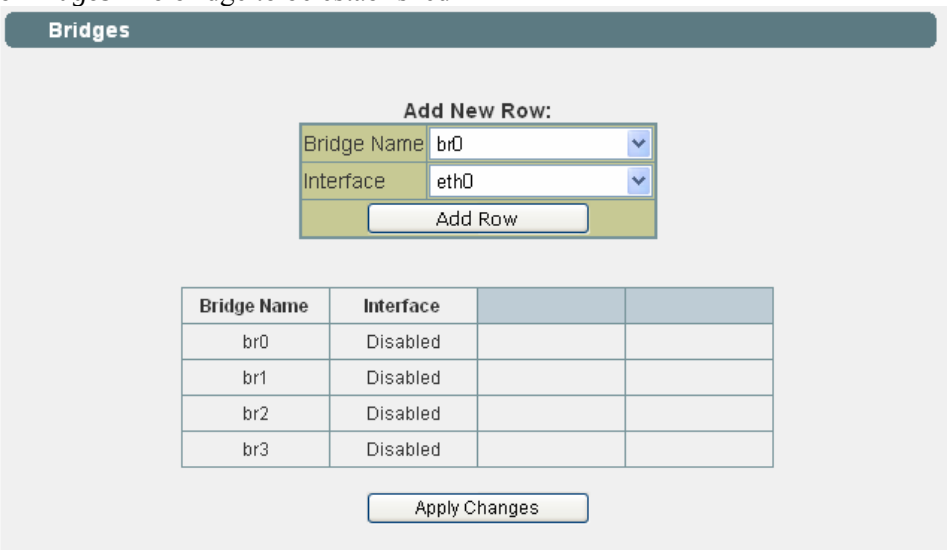
For Ethernet interfaces, you can also specify whether to connect to your ISP use PPPoE username and password. PPPoE login is executed when the option *Requires PPP login* is selected.

4.8 Connection Bridge, clustering Interfaces into bridges

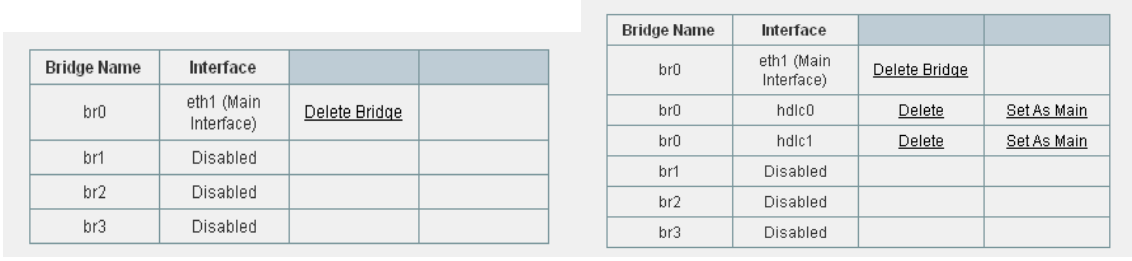
The router allows you to merge any number of Ethernet Interfaces in bridges. Network interfaces connected in the bridge mode behaves like a network interface. All packets that come to one of the bridge interface are sent to all other interfaces bridge, if, of course, are not addressed to the router.
To combine several interfaces into one, you should:

- Enter to tab *Bridges*
- decide which interfaces will connect to each other (eg eth1, hdlc0, hdlc1 connect the bridge br0).
- to an empty bridge table add an interface after which a bridge inherits the network settings
- to already created bridge with only one interface add extra interfaces
- after creating all bridge connections, select "Apply Changes". If interface you get the router is one of the main interface of one of the bridges, we do not lose connection with the router because settings of this interface will be moved to the settings of the bridge.

Empty tab *Bridges* - no bridge to be established



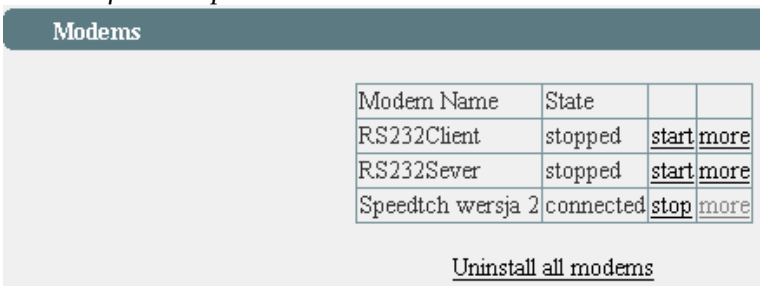
After you create the bridge, br0 bridge is exactly the same, but until now has been eth1 interface (left picture), after the addition of interfaces hdlc0, hdlc1 (configured in the mode hdlc-eth), br0 consists of three interfaces. br0 IP address, is set as before, to the address taken from eth1 when you create the bridge.



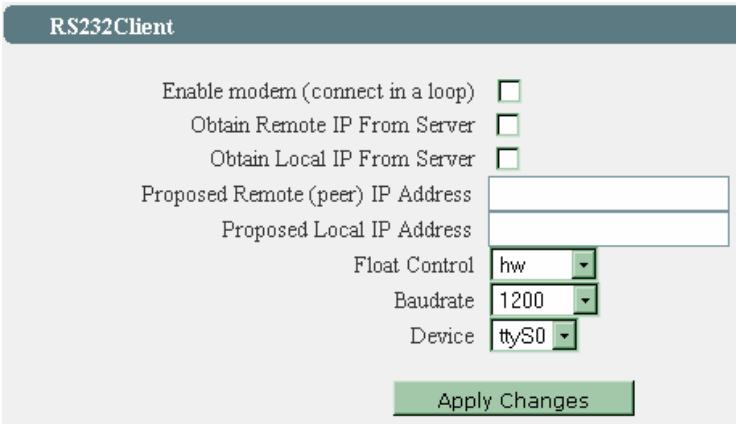
The bridge is treated from now on in the system as an interface br0. If you want to use a bridge connection, you must first compile and then configure the rest of the software.

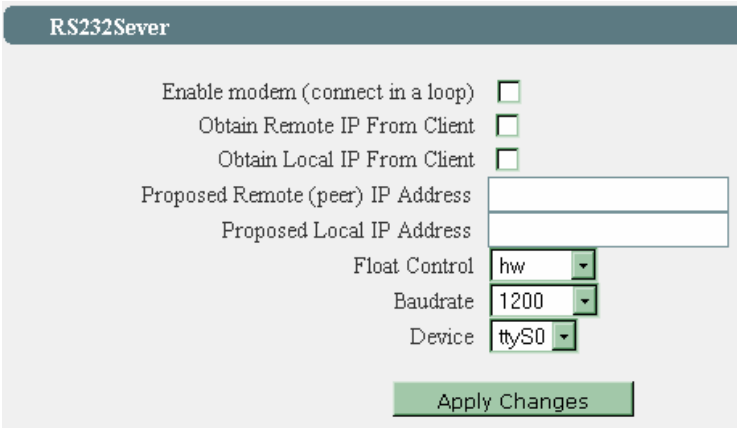
4.9 Configuring Modems

Currently supported modems are visible in the *Modems* tab. *Modems* tab and using modems has been implemented in this way, so you can easily add new modems. Support for new modems can be added to the software tab *Software Update*.



For modems understand the hardware that is supported by applications pppd. Modems are visible in the interface as a device ppp0, ppp1, etc.
Traditional modems can be supported by built-in RS-232 ports, with speeds from 1,200 to 921,600 bits/s





By default, the router is installed modems 232 Server - which allows you to receive connections via RS232 and RS232 Client - that lets you connect over the RS232 connection to your router on which is running the modem 232server.
The connection using the GUI can be compiled only on port ttyS1 - because port ttyS0 are used for logging by the RS-232 console.

4.10 Configuring access gateways: Gateways, Complex Gateway (load balancing)

Computers that provides the Internet are called "gateways." The graphical interface allows you to operate at Internet gateways as defined in the tab *Gateways* and the gateway "Gateway Complex" as defined in the *Complex Gateway* tab. Gateways defined in the tab *Gateways* called simple gates, the gate defined in the *Complex Gateway* gate complex. Gateways easily define Internet access points, the complex gateways allows access to internet by several gateways simultaneously.

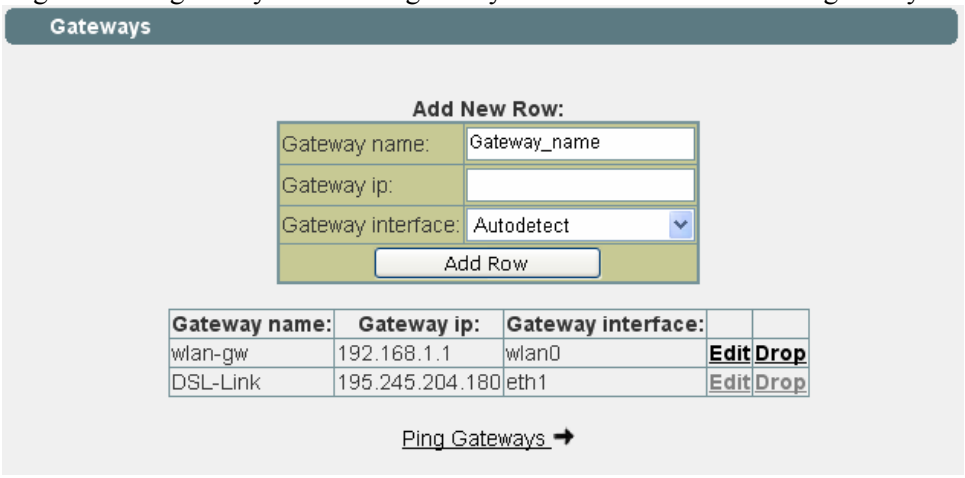
4.10.1 Defining simple gateways.

Each Internet gateway must have its own unique name in the system. You can not define the two gates of the same name, because an interface could not choose, which gateway to use. Each gateway, we can assign an IP address. We can assign the same IP gateways with different names, if we consider that this will help us setup. For each gateway, we can also specify a network interface, in which they work. If there is no need for attachment to a particular gateway network interface and gateway IP address uniquely identify a network interface gateway - we can choose an automatic search of interface, setting the field of *Gateway Interface* to *Autodetect*

Table: editing form fields of a single access gateway to the Internet..

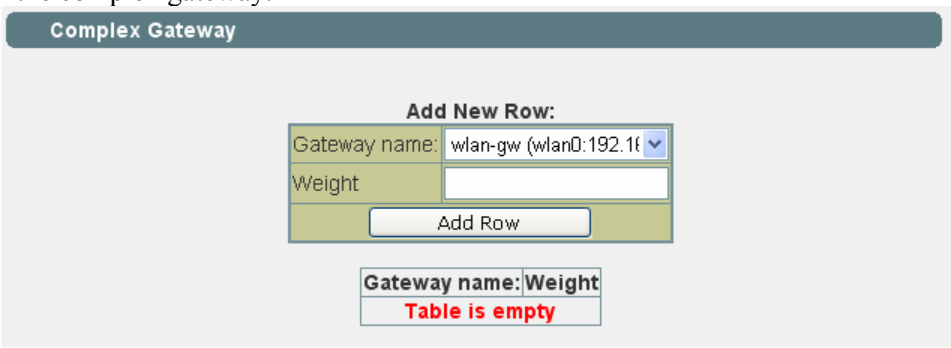
Field	Possible values	Description
Gateway Name	A string, without spaces, characters containing the English alphabet, numbers, and minus signs '-' and emphasize '_'.	The name used to identify the gateways in the configuration implemented by the GUI.
Gateway IP	The IP address, no spaces.	IP gateway, which inscription apply
Gateway Interface	Autodetect or an inscription that identifies the network interface	Allows you to attach the gateway to the interface, useful when you want to connect a gateway to a specific interface.

Sample configuration of gateways: the basic gateway WLAN and the additional gateway: DSL



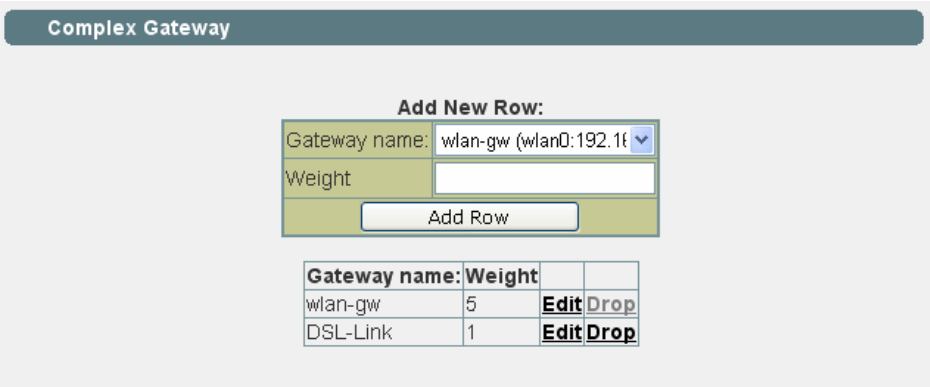
4.10.2 Complex gateway

Define a complex gateway building list of simple gateways from which it is made. Make selection through tab *Complex Gateway*. After entrance to the tab you see the form of a new gateway, for construction of the complex gateway.

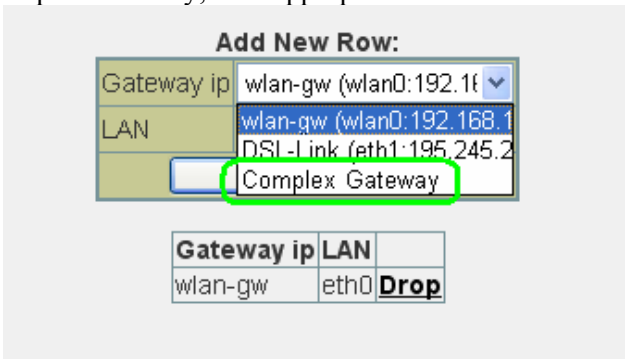


In the Gateway name will be able to choose the gates of the *Gateways* tab to be part of a complex gate. In the *Weight* field, we provide a number that will be the weight of the gateway. **Gateway weight** determines its capacity, in proportion to the other gateways in the system. If we define two gateways, one weighing 10, second with a weight 1, is the first of which will be sent to the 10 times more packages (the gate will be treated as 10 times more efficient).

When we have two connections to the Internet, for example, the main WLAN connection, a second slower DSL, but I would like to see both of these connections were used, it must first define them in the *Gateways* tab (as in the example in point. 4.10.1), and then both the gateways to add that just builds the table, to form a complex gate. In our example, DSL is 5 times slower than a link based on the WLAN:



To use the complex gateway, set the masquerade between LAN from which you want to use and complex gateway. In a list of access gateways in the *Routing/Masquerade* tab will have to choose the gateway "Gateway Complex". After its selecting, the traffic sent by all the gateways will be added to the construction of the Complex Gateway, with appropriate distribution.



Public Address IP field is used to enter the address, which will check the work of the gateways included in the complex gateway. Router at a time will perform PING public IP address by different gateways. If one loses the connection to the public IP address will be regarded as inactive.

4.11 Configuring Routing

In the current version of the graphical user interface routing is enabled between each pair of running network interfaces. On the *Routing/Masquerade* tab, masquerade can be defined between the networks indicated a network interface, and the selected gateway. Tab *Routing/Static* allows you to set static routes to the specified computers/computer networks.

4.11.1 Routing / Masquerading

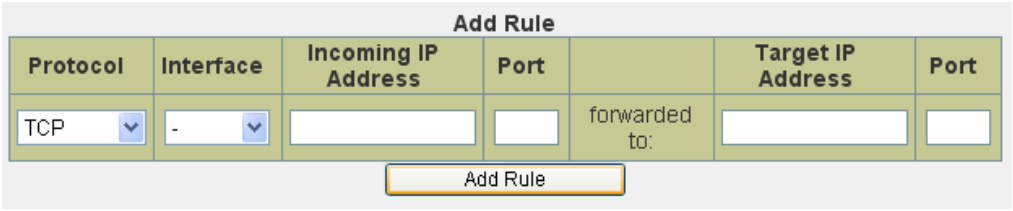
Masquerading allows you to share an Internet connection among multiple computers retracted behind a router - Gateway. In this configuration, the computers on the LAN communicate with the router, which forwards the query. The external network are shown as incoming queries from the router (hence the name: The Masquerade). Computers with the external network does not have direct access to computers on the LAN. Can get only to selected ports and the computers specified in the *Port Forwarding* tab.
In the gateways to choose from is also a gateway Complex Gateway. This means that traffic will be send from the router over several gateways simultaneously (load balancing) from among the appropriate distribution over the gateways. Gateway Complex Gateway is defined in the *Complex Gateway* tab, described in the point 4.10.2.

4.11.2 Routing / Static Routes

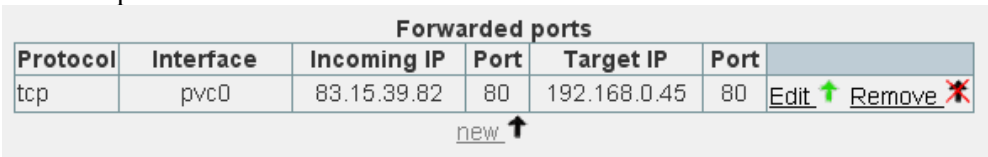
Tab *Routing /Static* allows you to specify so. static routes. Tab allows you to define to which network interfaces to route packets to be sent to selected IP addresses.

4.12 Setting up redirects (port forwarding)

Port forwarding and addresses redirection allows for access of computers of local network for users of the external network. Redirection is the combination of an incoming address (*Incoming IP Address* and incoming port (*Port*) to the addresses on the LAN (*Target IP Address/Port*). Port forwarding is set with a list of rules that you can add and edit using the form available on the table and the *Port Forwarding* tab.



In this example, web server set up on the local network at 192.168.0.45 is available on the external network, also known as a Web server, only globally accessible address 83.15.39.82. Router forwards packets addressed to him (83.15.39.82) that come to port 80 to the web server on your local network, then transmits a response



Of course, that the operation was successful, the router interface should be assigned to the incoming address "83.15.39.82".

4.13 Configuring the Firewall

Firewall is designed to block unwanted traffic packages. GUI allows the blocking of packets addressed to the router, and packets that the router is to redirect. Blocking packets is achieved by Linux *iptables* tool. Blocking packets passing through a router configure the firewall using a tab *Firewall/Forward*. Blocking packets addressed to the router configure using tab *Firewall/Input*.

4.13.1 Blocking packets passing through a router

After entering the tab *Firewall/Forward*, we can determine what kind of packages can freely pass through the router, which should be blocked.
At the beginning we define one of the strategies for packet transmission: all pass, and the selected block, or at first glance more restrictive: block all, transmits selected. Strategies for choosing the field value is defined: *Firewall Forward Chain default policy*. Selecting *Accept* means that packages that are not caught by the rules of the *Firewall (…) default Policy* option will be passed through. Selecting *Deny* option will see that if the package does not meet any of the criteria set out in the table of rules to block/transmission package - the package is stopped.

Table of rules to block/transmit packets edit like any other table by adding/editing lines with a green form of editing and watching the results of his work at the bottom of the page. The difference between this table and the majority of the table configuration is that it is **important in this sequence of rows.**

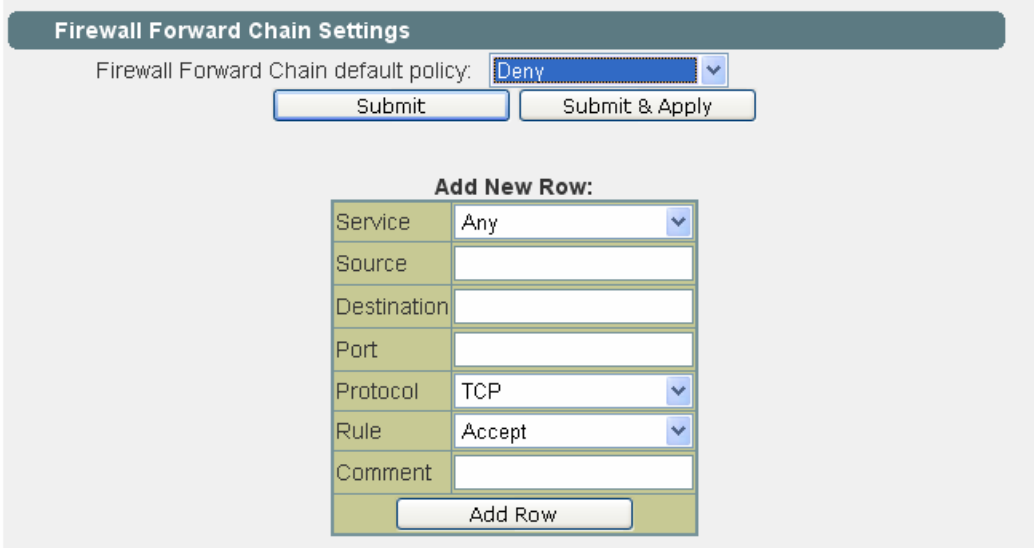
Each row defines the criteria package. Each package, before it is passed on through a router, you must first be matched to the criteria in different rows of the table, from the first row at the top, the last at the bottom. In addition to the criteria in each row is entered in the rule to be applied to the package that meets the specified criteria. The first line, which meets the criteria that are analyzed in the package - will include a rule that is applied to the package.

The most restrictive criterion for the time being you can specify:

- IP address/addresses of the sender of the package,
- IP address/addresses of the recipients of the package,
- the port to which the packet is routed
- the protocol by which the packet is sent (TCP/UDP/ICMP)\

The most universal criterion is to be met by all the packages: *Source: all, destination: all, Port: all, Protocol: ALL.*
For these criteria, use one of two rules: that accepts - *Accept* or reject: *Deny*. In addition, each line can indicate a comment.

An interesting field in the table is a field *Service*. This field is designed to relieve us from having to enter manually the port and protocol. Selecting a package that service *http* will block traffic packets TCP on port 80 *Port* and *Protocol* fields are taken into account only if the *Service* field is set to *Custom*.

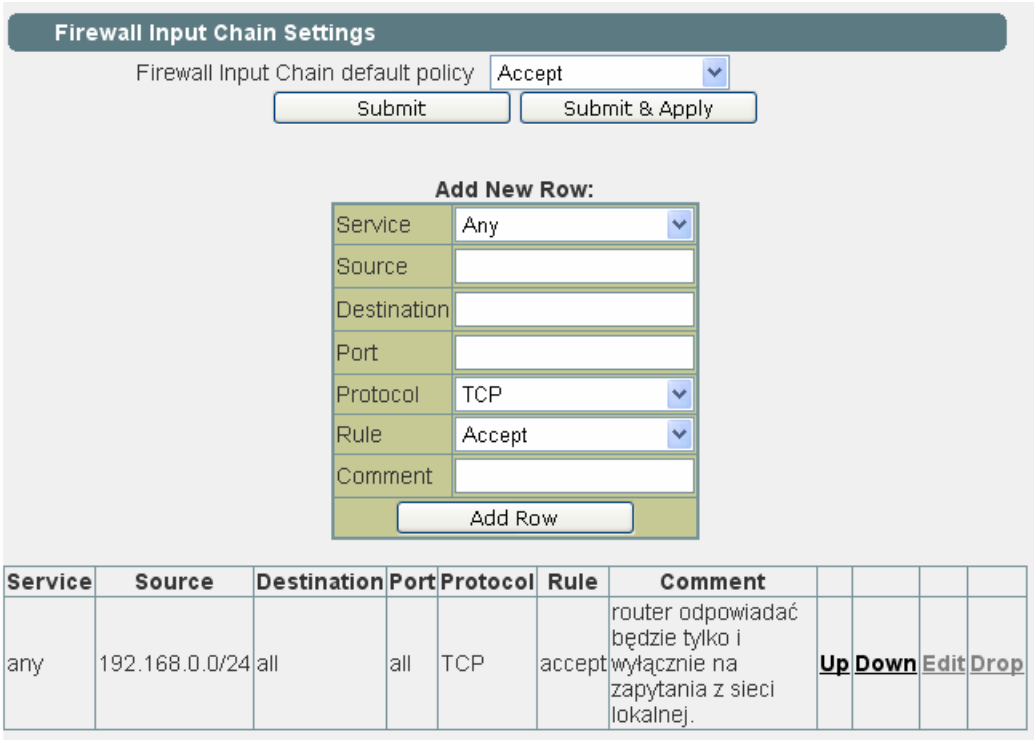


Service	Source	Destination	Port	Protocol	Rule	Comment				
any	192.168.0.0/24	all	all	TCP	accept	pozwalamy komputerom z sieci lokalnej komunikować się ze światem	Up	Down	Edit	Drop
any	195.245.245.204/30	all	all	TCP	accept	pozwalamy komputerom z odległego oddziału firmy na dostanie się do naszej sieci.	Up	Down	Edit	Drop

4.13.2 Blocking packets addressed to router

Packets addressed to the router are filtered via a tab *Firewall/Input*. The packet filtering rules are the same as the packet filtering rules to be redirected - the only difference is the use of the filter. If the package is not passed through the filter - the software (except, of course, software firewall) on the router will not get the information that the package arrived at the router. We can thus either block all attempts to contact the router from the external network, or vice versa - to designate the computers from which we can only get to the router.

In order to learn the rules of configuration, you should refer to the section 4.13.1. **We recommend caution when configuring this tab - you can, because in a very effective way to deprive the possibility of remote configuration of the router. In this case it will be necessary to login over the RS-232 console.**



4.14 Traffic Manager - limiting bandwidth

Traffic Manager tab allows you to limit bandwidth transmission of data to selected users. Functionality to configure by entering the table limits the amount of transferred data and the criteria for computers, these limits apply. In each row of the table are the criteria for determining the computers affected by the limitation contained in the row. These criteria are the IP addresses of computers or the MAC address of a particular computer. In the *IP Address* field, define a specific IP address or their entire class by adding "/" + netmask bits quantity. If you want to criterion was met by any IP address - enter „*". In the *MAC Address* field you can enter „*", address 00:00:00:00:00:00 or particulars computer MAC address, which alone is to meet the criterion of limitations.

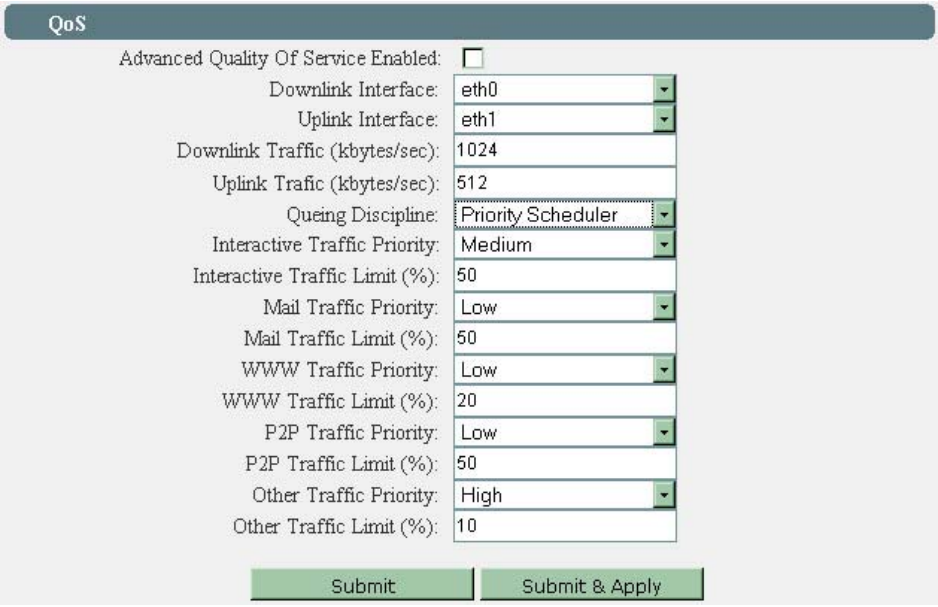
Bandwidth limit specifying how much data can be downloaded within seconds for computers meeting the criterion (downlink), how much data can send per second (UpLink), and how many packets per second can (together) to send and receive. Inserting the value of „0" will limit will no longer exist (if we wanted to block the route packets to the computer, use the tab *Firewall/Forward* (point 4.13.1).

Field	Acceptable Values	Field description
MAC Address	„*" or a specific MAC address of specific computer in the format XX: XX: XX: XX: XX: XX, where XX is a hexadecimal number.	„*" - indicates that the criteria for verifying the router does not pay any attention to the MAC Address, enter your address causes of choosing a particular computer.
IP Address	A specific IP address or class (network) IP addresses as IP / MASK (eg: 192.168.0.0/24)	Selects computers to limit bandwidth by IP addresses.
Protocol	You can choose the value of the TCP, UDP, ICMP, and ALL	Determine which protocol is specifically restricted
DownLink (kbps)	0 – 999999	How many kilobits per second can receive computers meeting the criterion
UpLink (kbps)	0-999999	How many kilobits per second can send computers to satisfy the test.
PPS (Packets Per Sec.)	0-99999	How many packets per second can send and receive computers that meet the criterion
Comment	A string of 64 characters	Comment

4.15 Quality Of Service - improving the quality of service

The mechanism of QOS (Quality Of Service) provides:

- Limit movement of the "downlink" – the quantity of data collected on the specified interface designated as the „*DownLink*".
- Limit movement of the „uplink" – the quantity of data collected on the specified interface designated as the „*UpLink*".
- The division into five streams of traffic based on the type of traffic.
- The ability to assign a separate priority for each band.
- The ability to assign a percentage of the declared use of bandwidth for each stream.
- Choice of limitations - a restriction of " unchanging" or "to lending".



4.15.1 Limitation "to lending".

If the options "Queing Discipline" is set to "Priority Scheduler" choose a restriction "to lending." In this situation, the router does not pay attention to the limit set as a percentage of bandwidth, if necessary using the entire bandwidth is adequate only if the number of packages.

4.15.2 Limitation " unchanging "

If the option "Queing Discipline" set to "Traffic Limiter", we can enforce that the stream does not exceed a "%" whole band. This may cause that part of the band is not used, but thanks if we have to send packets from another stream, you will not have to expect a release until the band. This may in some cases to reduce delays on the network - at the time of the connection.

4.16 Services "Services"

S*ervices* tab allows you to Specified services that can be used later in the *Firewall* tab. Services are generally understood as a couple: port / protocol. For example, we understand the HTTP service port 80 TPC. For an HTTPS understand port 443/TCP. But we can define a Web service and set that the will be blocked port and 443/TCP 80/TCP.
As defined then we can use the services in the tab *Firewall*, which will increase the transparency of the configuration.

Edit services by adding / removing rows from the table defined services. The services are distinguished the following protocols:

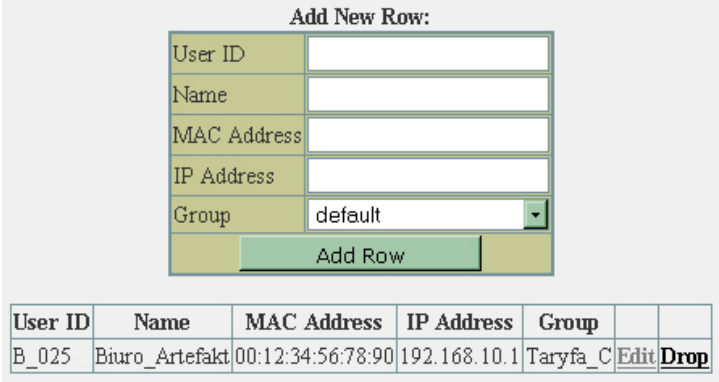
TCP (*Transmission Control Protocol*). TCP is a protocol operating in client-server mode. The server waits for connection on a particular port. The client initiates a connection to the server.
In contrast to UDP, TCP provides higher layers of communication to provide all the packages in their entirety, in the order and without duplicates. This ensures a reliable connection at the expense of increased overhead in the form of a header and a greater number of forward packets

UDP (*User Datagram Protocol*). This is the protocol without connection, so there is no charge to make connections and track sessions (in contrast to TCP). Nor is there any mechanisms for flow control and retransmission. The benefit of such a simplification of the construction is faster data transmission and no additional tasks which have to deal with the host using a protocol. For these reasons, the UDP is often used in applications such as videoconferencing, streaming audio on the Internet and online games, where data must be sent as soon as possible, and error correction are different layers of the OSI model.

ICMP (*Internet Control Message Protocol*) It is used in diagnosing networks and routing. Essential function in the control of the transmission network. Programs used in ping and traceroute.

4.17 Users

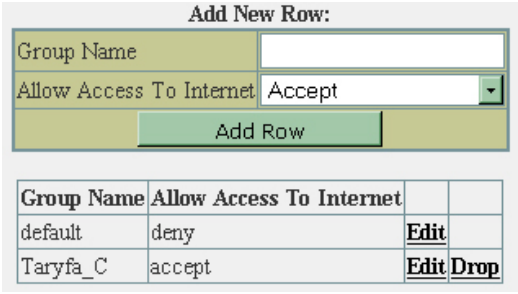
Users tab allows you to pursue a policy of sharing links and services for an individual user. In order to facilitate the management of users can be combined in the group



There we have the following fields:
User ID - used to link with other systems
Name - according to custom fields can be added to the group and check its operating statistics.
MAC address - to identify a user by MAC address
IP address - to identify a user by IP address
Group - the name of the group is assigned a user

4.18 Groups

Tab *Groups* lets you add new groups to which in the *Users* tab, add each user, making it easier to manage the parameters for access to Internet users.



Groups are used in the tab *Movement Manager*

4.19 Statistics

Statistics tab allows assessment of the overall system load.

Memory Free:	91356 kB
CPU Usage	0 %

Interfaces statistics

Interface	Received				Transmitted				Transmitted packets collisions
	Bytes	Packets	Packets with errors	Dropped packets	Bytes	Packets	Packets with errors	Dropped packets	
eth0	6M	34k	0	0	23M	29k	0	0	0
eth1	2M	3k	0	0	881k	3k	0	0	0
eth2	14M	95k	0	0	101M	105k	0	0	0
wlan0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0
hdlc0	0	0	0	0	0	0	0	0	0
hdlc1	0	0	0	0	0	0	0	0	0
ppp0	121M	138k	0	0	19M	127k	0	0	0

Reset Statistics

4.20 Hourly Statistics

Hourly Statistics show traffic on different interfaces in hourly intervals.

Interface: **eth1**

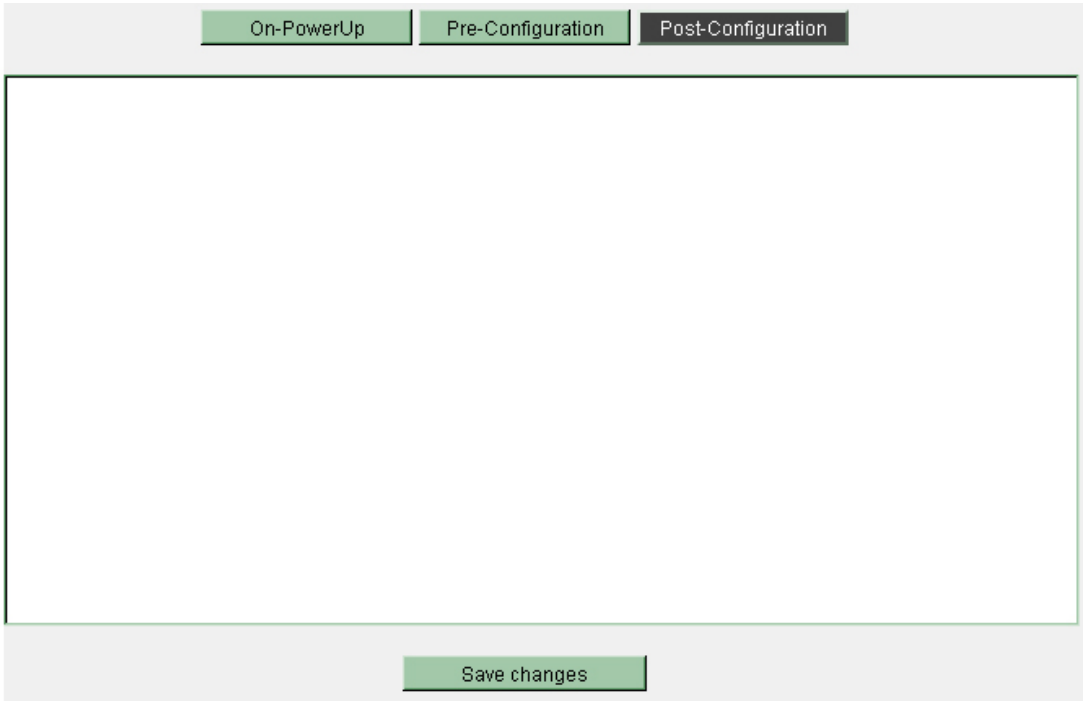
Hour	Average		Maximum		Hour	Average		Maximum	
	Rx b/s	Tx b/s	Rx b/s	Tx b/s		Rx b/s	Tx b/s	Rx b/s	Tx b/s
0:00 - 0:59	0	0	0	0	12:00 - 12:59	0	0	0	0
1:00 - 1:59	0	0	0	0	13:00 - 13:59	9	48	77	419
2:00 - 2:59	0	0	0	0	14:00 - 14:59	0	1	9	19
3:00 - 3:59	0	0	0	0	15:00 - 15:59	0	0	0	0
4:00 - 4:59	0	0	0	0	16:00 - 16:59	0	0	2	1
5:00 - 5:59	0	0	0	0	17:00 - 17:59	4	23	52	284
6:00 - 6:59	0	0	0	0	18:00 - 18:59	7	45	70	407
7:00 - 7:59	0	0	0	0	19:00 - 19:59	0	0	0	0
8:00 - 8:59	0	0	0	0	20:00 - 20:59	0	0	0	0
9:00 - 9:59	0	0	0	0	21:00 - 21:59	2	12	22	106
10:00 - 10:59	9	138	57	1k	22:00 - 22:59	3	20	26	165
11:00 - 11:59	13	78	73	454	23:00 - 23:59	0	0	0	0

4.21 User Statistics

Tab allows you to observe the traffic generated by a single user

4.22 Tab Configuration Script

The purpose of a graphical user interface is to allow the use of the basic functionality of the router, without having to manually write scripts. Since the user requirements can be very broad, it is possible to direct entry commands using tabs: Configuration Script, or by modifying the configuration scripts through the console (SSH functionality for more advanced users).


On-PowerUp
Pre-Configuration
Post-Configuration
Save changes

Typed scripts can be performed on one of three ways:

- On – PowerUp
- Pre – Configuration
- Post – Configuration, in this case the script complements the functionality of the GUI that is not supported

After entering the script, press the *Save changes* to make changes to the router's RAM that has been done to further press the *Apply changes*. In addition, the changes are saved after the power is turned off, press the *Write to Flash*.

4.23 Software Update GUI

Please download from www.goramo.com.pl current version of the graphical user interface. Put it on your computer to a directory whose full name does not include Polish characters and is not longer than 60 characters. Recommended is the main directory of a hard drive of your computer.
After recording the file, go to *Software Update* tab and using the *Browse* button, indicate the previously downloaded version of the graphical user interface. Then click *Software Update*. After loading the software into router RAM, a message indicates that the software was downloaded and asked to confirm your intention to update the software.
" *Successfully uploaded release-file, continue update?*"
Should be confirmed by selecting the button:
" *Yes, install New release* ".
The new software version will be recorded on the device. Now we can do nothing else but to see if it works - and if it works correctly - write to *Flash* memory by selecting: *Write to Flash*.

5 Manual MicroRouter text menu over the console (only for MicroRouter)

To fully exploit all the advantages and MicroRouter opportunities need to know Linux system. Starting in front of users, however, not know this system has been preset frequently used functions available via the console and the text menu:
1. Setting MicroRouter to work in bridge mode (hide the IP address)[2]:
   Eth: on both Modems, Converters E1etc. set mode "Bridge Ethernet (eth0) and over hdlc0 hdlc1"
2. Go to the router mode - that is, IP address and unlock the ability to configure the Web browser.
3. Go to the Linux system console mode - allowing the use of additional operating system functions not implemented in the version of the web browser configuration.
4. Log out

After connecting the console to a socket system asks the user for username and password (if the connection was held at the operating system, press Ctrl + D):

```
multilink login: root
Password: goramo1234
```

Message displayed when you boot the console port:

```
Welcome to Text User Interface (TextUI) of MultiLink-MR Router (Micro-
Router).
Chose option:

1. Set to and configure Bridge Operation Mode;
2. Set to Router Operation Mode;
3. Go to console;
4. Logout.
```

[2] It is point for two this same devices eg. Modems, Converters E1 installed on the link

When you select an Enter key and approval are two connection options:

```
Select bridge configuration  media to be bridged over HSS0 to DCE


1. Bridge Ethernet (eth0) over HSS0 (hdlc0 and hdlc1) - normal RxClk
2. Bridge Ethernet (eth0) over HSS1 (hdlc0 and hdlc1) - invert RxClk
```

The first combines all the interfaces in a transparent bridge (for Goramo Converters E0 and Goramo Converters E1). The second does the same, but for the HDLC interface uses a different clock edge (for Goramo Alfa2 modems). When set to enter the router configuration, and then asks whether you want to save the new setting in the flash memory:

```
The device configuration has been changed and applied.
Do you want to save changes into Flash memory?

(Y) Yes
(N) No
```

After selecting Y and approved, you will get the message:

```
Saving changes.
<wait>
```

Writing to flash memory takes about 40s. (This confirms LED Flash busy "), then a message is displayed:

```
Changes has been saved. Press <Enter> to go back to main menu.
```

After pressing Enter the main menu appears in the selection.

If you select the message N

```
Changes were not saved into Flash, they will be valid until rebooting
the device.
Press any key, to go back to main menu.
```

After pressing Enter the main menu there is a choice.

After entering changes to select option "4 Logout and log out of your system.

6 Upgrading the Linux operating system

Device's operating system is modified. The company's website: http://goramo.com.pl/public/, all the time for the latest version of the kernel. Users can independently perform router updates the version of the operating system without compromising the GUI version, or using the current configuration of RedBoot commands. RedBoot can to get the first 10 seconds after power is supplied only via the RS-232 console connected to the Control Port or port designated as ttyS0, depending on the version of your router.

For Linux operational system upgrading you should:

1. At the local server TFTP (Windows or Linux)[3] copy image file armeb* taken from GORAMO – Janusz Górecki (www.goramo.com.pl) or make by yourself
2. connect port Eth0 to TFTP server, and converter control port to PC computer RS232 port, where terminal program runs (for example: HyperTerminal – Windows or MiniCom – Linux, with following port setting: 115,2 kbit/s, 8N1, flow control: OFF or XON/XOFF).

[3] for example from the site www.chip.pl

Upgrading the operating system software is achieved through the program RedBoot over port Eth0 as follows: shortly after the RedBoot startup is running, which pre-boot Linux stops at 10 seconds, giving the possibility, among other things, delete the old files and download new. Bold in the following procedure, indicated the place in which to change or enter the appropriate value for its own network.

Attention!!!

Before deleting files by command fis delete you should check whether loading of files from server TFTP work; the best command is: `load -r -b 0x800000 gml*.img` – if the file has been loaded, the following message will be displayed: `Raw file loaded` ..... It was it been possible then to begin lower described procedure of actualization.

The procedure was it been possible to shorten to marked with **blue** color commands**,** if the setting of server TFTP will agreed from settings in RedBoot, in peculiarity: Default server IP address: **192.168.0.45**

```
RedBoot(tm) bootstrap and debug environment [ROM], Built Dec 18 2007

Platform: Router MultiLink (XScale) BE
Copyright (C) 2000, 2001, 2002, 2003, 2004 Red Hat, Inc.
Copyright (C) 2003, 2004, 2005, 2006 eCosCentric Limited

RAM: 0x00000000-0x08000000, [0x00024320-0x01fcd000] available
FLASH: 0x50000000 - 0x51000000, 128 blocks of 0x00020000 bytes each.
=Executing boot script in 10.000 seconds - enter ^C to abort
^C
RedBoot> fis unlock -f 0x50060000 -l 0xfa0000
RedBoot> fis delete router
RedBoot> load -r -b 0x30000 armeb*
RedBoot> fis create router
RedBoot> reset
... Resetting.
```

If everything went correctly there should be booting

You can change the address of the tftp server to another if it does not correspond to the factory setting, from within RedBoot

```
RedBoot> fconfig -i
Initialize non-volatile configuration - continue (y/n)? y
Run script at boot: t
Boot script:
Enter script, terminate with empty line
>> fis load router
>> exec
>> <┘
Boot script timeout (1000ms resolution): 10
Use BOOTP for network configuration: f
Gateway IP address: 192.168.0.1
Local IP address: 192.168.0.35
Local IP address mask: 255.255.255.0
Default server IP address: 192.168.0.45
Console baud rate: 115200
GDB connection port: 0
Force console for special debug messages: false
Network debug at boot time: false
Default network device: npe_eth0
Update RedBoot non-volatile configuration - continue (y/n)? y
... Unlock from 0x50fe0000-0x51000000: .
... Erase from 0x50fe0000-0x51000000: .
```

```
... Program from 0x01fe0000-0x02000000 at 0x50fe0000: .
... Lock from 0x50fe0000-0x51000000: .
RedBoot> reset
```

After this command, there should be a normal boot, you can also go to RedBoot
Useful commands:
`fis list` –shows the contents of Flash memory
`fis list -c -d` –shows the contents of Flash memory and Checksum

6.1 Create a copy of the operating system and configuration settings

In the directory
`/dev/mtd/IXP4XX-Flash.0`
Located a file (character device) with the whole 16 MB of flash files.

For example you can copy from him everything without RedBoot file:
`dd bs=$((0x20000)) if=/dev/mtd/IXP4XX-Flash.0 of=input_file skip=3`
In this way we write down flash image to RAM.

If we want to write down flash image to local computer we should execute on this computer following command:
`nc -l 1234 > flash_image`
and on router we execute:
`dd bs=$((0x20000)) if=/dev/mtd/IXP4XX-Flash.0 skip=3 | nc xxx.xxx.xxx.xxx 1234`
where: xxx.xxx.xxx.xxx local computer IP address and 1234 is the port number of this local computer

(skip=3 skips 3 RedBoot blocks, it means that specific setting for hardware router version are not copied.)

You can do the opposite direction (MultiLink routers only!):
`dd bs=$((0x20000)) of=/dev/mtd/IXP4XX-Flash.0 if=output_file seek=3`

For MicroRouter update have to use RedBoot application p.6

Warning!
Do not just wrong directions: `skip=X` skips blocks to the entrance,
`seek=X` starts recording from the block X to exit `bs=block size`, `if=input` file, `of=output file`. ???????

"`Read-only filesystem`" means that a block is protected
record, you need to do then RedBoot eg
`fis unlock -f 0x50060000 -l 0xFA0000`

dd output can also refer to the pipe (if we do not give of = XXX)
description is in google man dd.

6.2 Backup and Restore Features

The router's Flash memory has been set aside two areas of configuration:
- Conf (core area which is read the current configuration)
- Conf2 (additional area to which you can save the configuration of the reserve)
To save the current configuration in addition to conf2 area should be from the console command:

`/etc/UI/scripts/backupGUI`

To recover the reserve configuration is the console command:

```
/etc/UI/scripts/restoreGUI
```

Please note that in both cases, the entry to the flash memory must be unlocked.

7 Sample configurations

Fill the field so a DLCI value of Channel in 99 and select the button *Submit & Apply*. Configuring the device will be introduced at this point to use. If you have a problem with setting pvc0 channel (described below), try to change the slope of the clock signal sending / reading the data by selecting the appropriate clock. Such issues arise from the use by chip manufacturers

7.1 Setting up a VPN connection

The VPN connection, called the "tunnel" to connect with each other two distant local networks into one. First, we describe the simplest configurations, which are linked together two LANs. This configuration of the hardware is as follows:

Configuration Description:

Computers with LAN-1 enter the Internet through a router-1, computers with LAN-2, enter the Internet through Router-2. Both routers are assigned global IP addresses may be appropriate for the is 80.50.70.1 for router-1 and 80.50.80.2 for router-2.
LAN have addresses in the 192.168.1.0/24 pool for LAN-1, 192.168.2.0/24 for the LAN-2.
In the following chapter we consider the situation where we want to connect more LANs together multiple tunnels.

7.1.1 Connecting two LANs over one VPN tunnel

Each tunnel may connect the two LANs. Tunnel configurations we introduce the two routers - located at the end of the tunnel. Routers need not be the same, just the statement that the tunnel will use the same protocols.
We describe in detail the configuration of the router on one side of the tunnel, router configurations on the other side only to be presented.

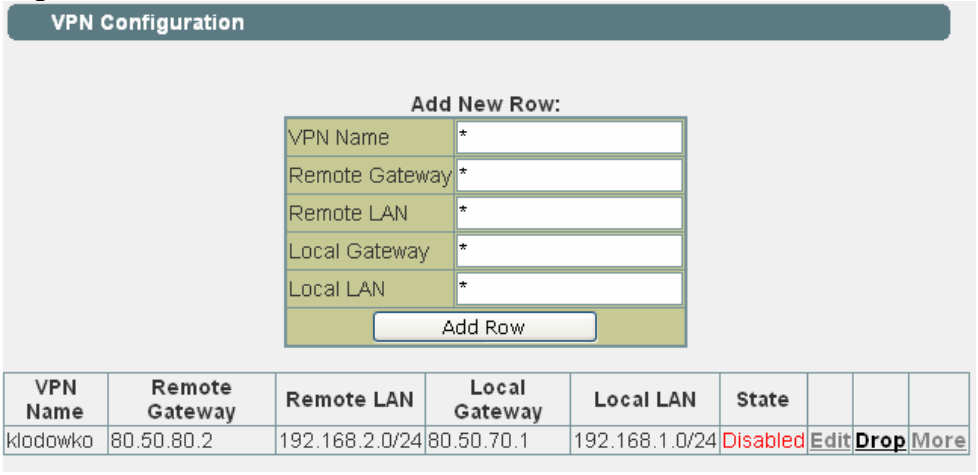
We go to the "VPN Configuration" and enter the initial configuration of the tunnel. Initial configuration - means following settings:

- **VPN Name:** the name of the tunnel,
- **Remote Gateway:** IP address of the router on the other side of the tunnel,
- **Remote LAN:** Local Area Network Addressing on the other side of the tunnel,
- **Local Gateway:** IP address that configure the router (the router can have multiple IP, so it should be used these which configure the VPN router and from which router is visible from the outside).
- **Local LAN:** network addressing configured on the router.

In the tab "VPN Configuration" we see a table of pre-configured VPN tunnels. In particular, this list may be empty. Add a new line stating the details of a new tunnel.
In the below example it will be (for Router-1 from the description at the beginning of this section):

field	value	description
VPN Name:	Krakow	For example, the name of the municipality in which the second end of the tunnel.
Remote Gateway	80.50.80.2	address ROUTER-2
Remote LAN	192.168.2.0/24	Network addressing LAN after ROUTER-2
Local Gateway	80.50.70.1	address ROUTER-1
Local LAN	192.168.1.0/24	Network addressing LAN after ROUTER-1

After entering the tab row to the table will look like this:



After initial setup the tunnel - go into configuration details - More choosing the right line.

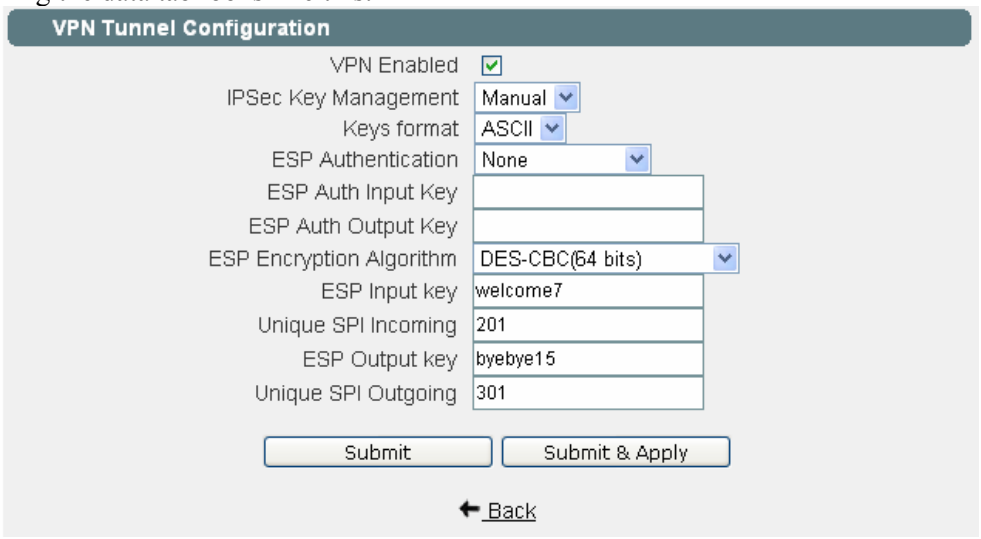
7.1.2 Details of the connection setup

After initial setup the connection (previous section), go to the configuration details. Details of these protocols are used for authentication and data encryption. On this tab you need to manually enter the keys used for encryption.

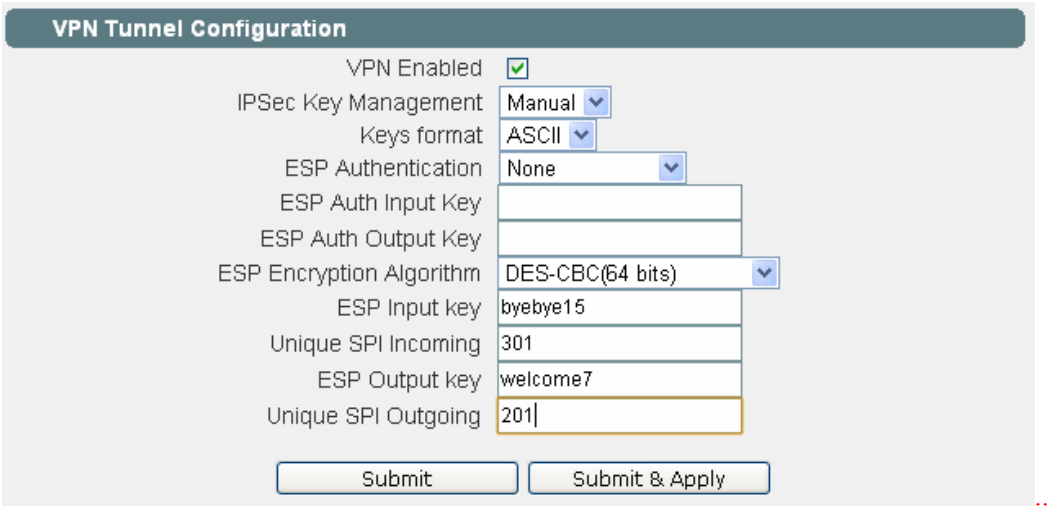
For the settings we have:

Field	Sample values	explanation
VPN Enabled	marked	The tunnel is to be run
IPSec Key Management	Manual	Manual key management, the user must manually enter the keys in the configuration tab.
	Auto	Automatic key management IS NOT IMPLEMENTED.
Key formats	ASCII	The keys (in the fields of ESP Auth. Input/ Output Key, ESP Incoming/Outgoing Key) enter in the form of text (ASCII)
	HEX	Introducing Keys as hexadecimal numbers
ESP Authentication	None	The field is not used. It is required for automatic key exchange.
	MD5(128Bits)	The field is not used. It is required for automatic key exchange.
	SHA1(160Bits)	The field is not used. It is required for automatic key exchange.
ESP Authentication Input Key	128 lub 160 bitowy klucz	The field is not used. It is required for automatic key exchange.
ESP Auth Output Key	128 lub 160 bitowy klucz	The field is not used. It is required for automatic key exchange.
ESP Encryption Algorithm	None	Danie nie są szyfrowane
	DES-CBC(64bit key)	64 bit DES algorithm. Requires the 8 characters in ASCII or hexadecimal number with a length of 16 characters
	3DES-CBC(192bit key)	192-bit 3DES algorithm (triple DES), requires 24 ASCII characters or 48 character hexadecimal number.
	RIJNDAEL-CBC(128bit key)	Rijndael algorithm with 128-bit key - requires 16 ASCII characters or 32 hexadecimal digit number.
ESP Input key	adequate number of characters, or a suitable length of a hexadecimal number, depending on the encryption algorithm.	key / password / for incoming data from the router on the other side of the tunnel
Unique SPI Incoming	triple-digit hexadecimal number from 001 to FFF	A unique identifier for the “tunnel coming"
ESP Output key	The key for outgoing packets	The password for the outgoing packets. It must include an adequate number of characters.
Unique SPI Outgoing	hexadecimal number from 001 to FFF	D appended to the outgoing packets.

After entering the data tab looks like this:



When you select Submit, and make changes (Apply Changes at the left-hand menu) or select Submi & Apply - router, comparing the tunnel. To operate the tunnel routers on both sides must be configured.

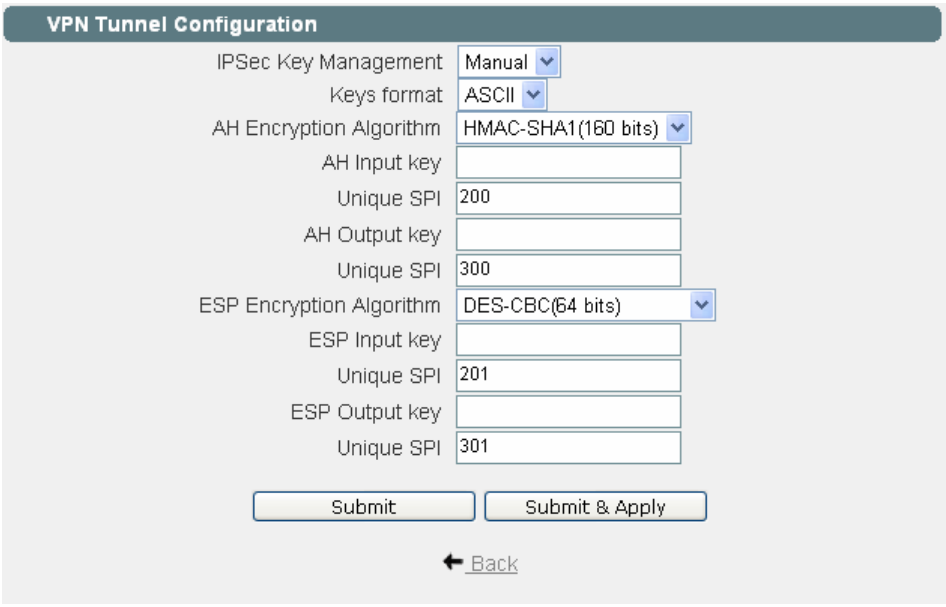


After administration of addresses on which the VPN tunnel is built, go to the advanced settings for the tunnel, the encryption algorithms used to select and enter keys. Once approved, the settings will be connected.

7.1.3 Configuration "other" side tunnel

For the configuration described above - fits symmetric configuration, as described below:

VPN Name	Remote Gateway	Remote LAN	Local Gateway	Local LAN	State			
warszawa	80.50.70.1	192.168.1.0/24	80.50.80.2	192.168.2.0/24	Disabled	Edit	Drop	More



7.1.4 Additional information on the implementation of VPN

To implement a VPN router uses an IPSec-tools package and its composition falls within the setkey tool. This tool is used for the compilation of the tunnel and accessible from the command line router. The current implementation only supports manual key exchange.

To check whether the tunnel works correctly, you can log into the router and send control packets (ping), first to the gate on the other side, then to the computers in local area networks.

Connection status can be monitored on the tab with a list of pre-configured tunnel (Field State - if it is to Enabled, the tunnel is working properly, Disabled - indicates that the tunnel is switched off or not tabulated).

Summary of the tunnel, you can check the command "setkey" (a detailed description of commands available on the Internet), call:

```
setkey -DP
```

This command writes a rule that configures a tunnel, and how much to use different rules (increasing volume of use shows that the router attempts to use the tunnel).

In case of troubles we suggest to see:

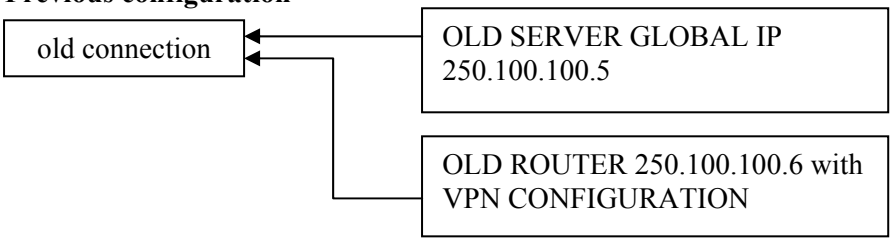
- SPI numbers match
- Key format
- IP addresses
- Web addresses whether they are in the correct format: xxx.xxx.xxx.xxx/yy
- LAN on different sides of a tunnel must have different IP addresses.

7.2 Transitive router

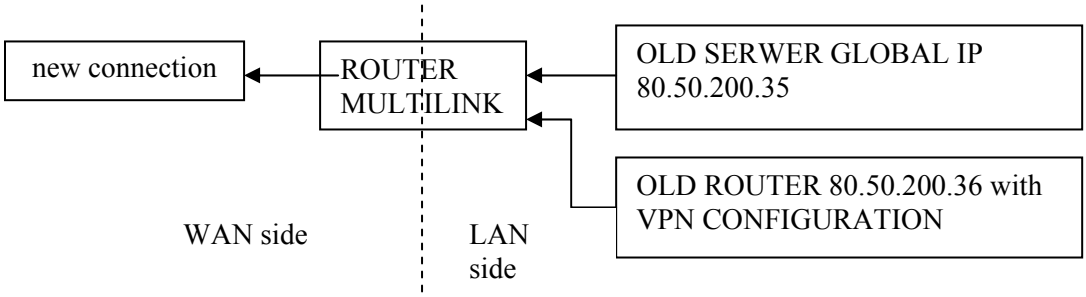
Frequent use of the router is working as an interface to link E1/V.35. Mostly this applies to users who run a network based on DSL, and wanting to get more bandwidth - exchanged on the connection speed POLPAK-T or faster connection.

Since the router requires only that he mediated possibly transparently link between the new and pre-configured computers / routers that were previously assigned global addresses. Unfortunately, in most cases you must change the global addresses assigned to computers configured already - but it's usually easy requirement to meet.

Previous configuration



Desirable configuration with the division to the WAN and LAN



The desired configuration is shown in the preceding paragraph of this diagram. In this configuration ROUTER MULTILINK on the WAN side has to communicate with a gateway of ISP Gateway and on the LAN side has to communicate with our computers. LAN side is all what we have physical access. WAN side it is link and a network interface connected to the interface - the rest of the WAN - is at the ISP.

The router communicates with the Internet provider working in the WAN (one of its interfaces, mostly HDLC, or PVC) is often called in network as router subscriber network - which is a network which operates an ISP gateway. In the LAN, router is working together with the "old" devices.

In each network the router must have an IP - matching network. "Old" devices must have IP addresses that match the LAN and globally. Router on the LAN side must have a matching IP to the LAN. WAN-side router must have a matching IP network which operates an ISP gateway.

Since the routing between all network interfaces by default is available, the WAN router transmit all packets addressed to devices with global addresses on the LAN. ISP Gateway will be the default option for packets addressed to the "other" computers; packets of global addresses will be routed to the ISP. Nothing but a network address assignment is not needed.

For example, when we are dealing with a link POLPAK-T we obtain the addresses of connecting networks, such as:
80.50.70.30/30
ISP gateway is available in the: 80.50.70.31
Dedicated is the IP address for your router: 80.50.70.32
I assign these addresses the WAN interface and enter the Gateways tab. If the globally allocated / 29 (Other than the Web connection!)
One of them is excreted for the router, and the rest split between the old device. Enter configuration into tab Interfaces for port Eth0 or Eth1 (according to which we are connected to the LAN). Nothing more to be done - just make sure that the Firewall tab is not blocked for unwanted traffic packages - Default Policy: Deny - should be changed to ACCEPT.